



WHITE PAPER

SHINING A LIGHT ON THE GLOBAL BULLETPROOF HOSTING ECOSYSTEM



TABLE OF CONTENTS

Executive Summary	1
Key Findings	2
What is a Bulletproof Hosting (BPH) Provider?	3
How BPHs Get Online	4
The Silent Push Process for Identifying BPHs	5
Actionable Queries & Red Flags for Defenders to Investigate	20
AS Number: 152194 (AS Name: CTGSERVERLIMITED-AS-AP)	20
AS Number: 214351 (AS Name: FEMOIT GB)	22
AS Number: 213194 (AS Name: NECHAEVDS-AS RU)	23
AS Number: 215789 (AS Name: Karina Rashkovska)	24
AS Number: 214943 (AS Name: RAILNET)	25
AS Number: 34985 (AS Name: NETINNOVATIONLLC-AS-AP)	25
AS Number: 48589 (AS Name: SOW-A-AS UA (Also known as "Tiger Net"))	27
AS Number: 49217 (AS Name: HOSTYPE US)	27
AS Number: 214940 (AS Name: KPROHOST LLC)	29
AS Number: 140224 (AS Name: SGPL-AS-AP STARCLOUD GLOBAL PTE. LTD. SG)	30
Other Types of Bulletproof Hosting	32
Infrastructure Laundering: The Next Step for Bulletproof Hosting Providers	32
Dynamic DNS (DDNS) Providers Create BPH-Like Networks	33
Bulletproof Registrar: NiceNIC	34
Increasing Pressure on BPH Providers Using Government Sanctions	35
Bulletproof Hosting is Expanding, Not Going Away	36
About Silent Push	37

EXECUTIVE SUMMARY

Bulletproof Hosting (BPH) providers have been a part of the threat actor landscape for over two decades. However, the market has experienced a renaissance in the last year. A surge in providers globally, an evolution in new tactics, and increased resilience against takedown efforts have highlighted just how deep and murky this space has become from a defender's perspective.

Silent Push offers this white paper to not only illustrate the current state of play in the practice of Bulletproof Hosting providers (BPHs), but also to highlight the potentially lesser-known technical dynamics we've been seeing in the background. Our world-class threat analyst team has been hard at work, providing and scaling our detection of BPH infrastructure, so that our clients can utilize those detections within their Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tooling for accurate, dependable alerting on suspicious and malicious activity.

Colloquially, internet hosting service providers were labeled "Bulletproof" for their willingness to host services that were specifically designed to shield clients from technical and/or legal disruption. Our researchers employ a wide range of criteria to label the hosts we track as bulletproof, many of which we will cover in detail in this report. Some, however, we cannot disclose for operational security reasons. We believe that sharing these criteria and methods publicly is crucial in informing defenders about where cybercriminals are hiding their networks.

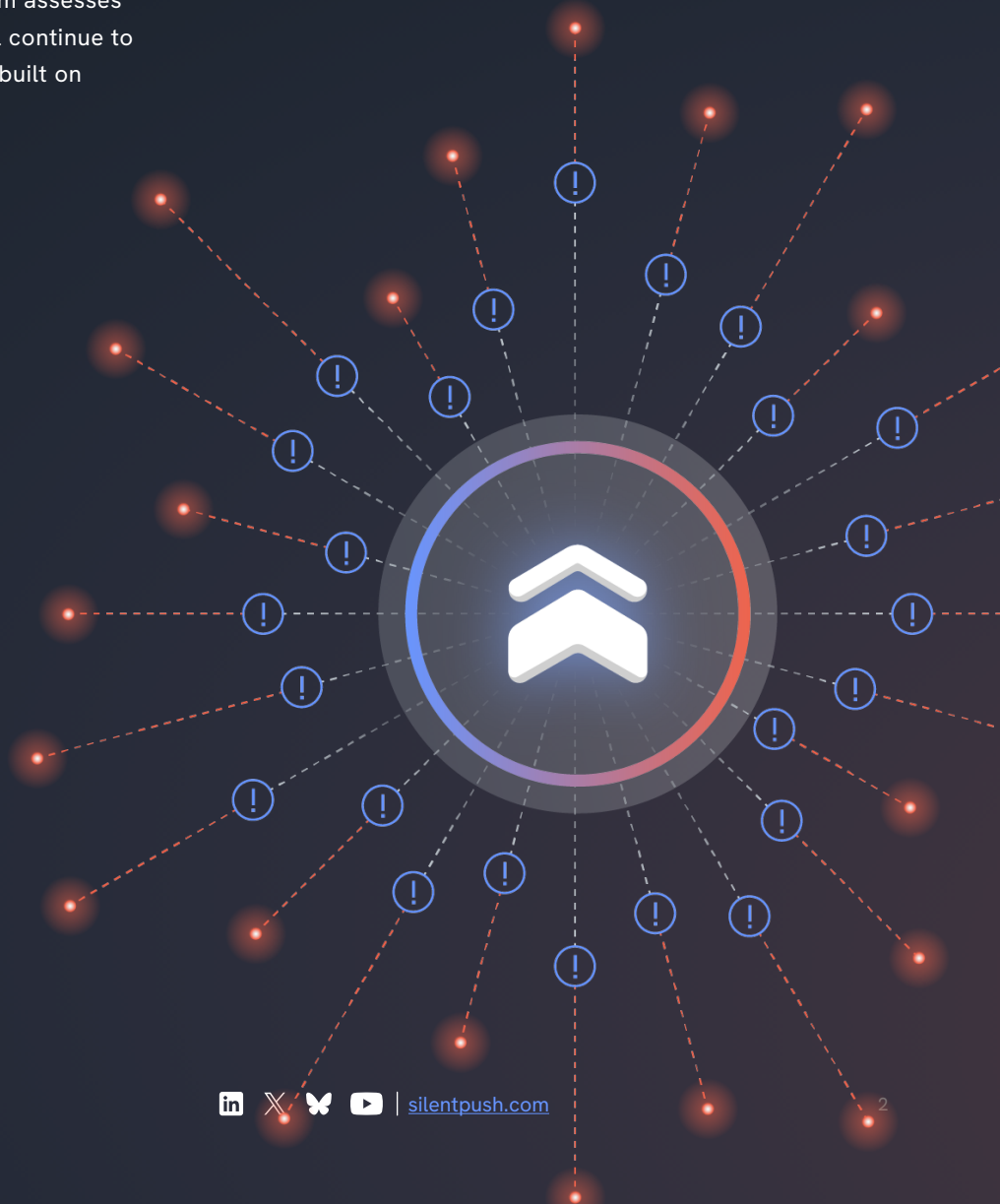
With the rise of artificial intelligence (AI) and large language models (LLMs), we anticipate that threat actor automation of infrastructure setup will continue to increase into 2026 and beyond. Extensive coverage of BPH providers enables defenders to maintain awareness and alert on suspect infrastructure that is frequently used for obfuscation and weaponization, ensuring that actors using these networks as part of their automation fail before they can initiate attacks.

By circulating this information publicly without restriction, our goal at Silent Push is to reach communities that have the means and motivation to shape a safer, more accountable cyber threat landscape, with preemptive cyber defense for threat hunters, policymakers, researchers, journalists, and government teams.



KEY FINDINGS

- Threat actors are drawn to Bulletproof Hosting (BPH) providers for their permissive policies regarding hosted content and their hands-off approach to abuse complaints and takedown requests. These providers allow malicious infrastructure like phishing kits, Command-and-Control (C2) servers, or dataexfiltration points to remain online longer with fewer disruptions.
- Cybercriminals leveraging BPH infrastructure move faster than defenders can respond, often migrating operations, re-registering domains, and re-establishing services within hours of takedowns. Without knowledge of where this infrastructure shifts, takedowns lack the permanence they need. And without a coordinated shift in both regulatory pressure and the law-enforcement action aimed at these providers, our team assesses that Bulletproof Hosting as a service will continue to thrive—as will the malicious operations built on top of it.
- Silent Push provides defenders with exactly what they need: real-time data and hunting tools to block malicious traffic emanating from BPHs. Our **Indicators of Future Attack™ (IOFA™)** feeds for BPHs are explicitly designed to expose threat actors as they migrate their infrastructure, flagging new ASNs, IP ranges, and hosting providers long before they appear on other threat radars. We actively monitor more than 200 BPH providers—a number that increases nearly every week—and the ASNs used to collectively control broad swaths of the internet. Our platform features an ever-increasing catalogue of SIEM, SOAR, and other integrations to support organizations' need for preemptive defense; the current list can be found [here on our website](#).



WHAT IS A BULLETPROOF HOSTING (BPH) PROVIDER?

The term “bulletproof hosting” first appeared in 2006 to describe infrastructure operated by the [“Russian Business Network,”](#) a notorious provider known for hosting large-scale phishing and malware campaigns that [reportedly](#) defrauded victims of roughly \$150 million. The phrase caught on in cybersecurity circles before reaching mainstream audiences through [a 2007 Washington Post exposé](#) on the network’s role in global cybercrime. Today, “Bulletproof Hosting Provider” is an industry fixture, cited across threat intelligence reports and reflected in public resources such as Spamhaus’s Don’t Route or Peer (DROP) ASN list of known BPH networks.

Put simply, a BPH refers to any hosting provider that ignores, resists, or otherwise fails to respond to legitimate abuse reports. Unlike legitimate providers who are incentivized to swiftly disable malicious infrastructure, BPH operators delay, dismiss, or deliberately ignore such reports, creating environments where threat actors can operate with impunity. Each ignored complaint extends the life of this malicious infrastructure and fuels a perverse feedback loop—one where criminals finance the very hosts that protect them, and both sides profit from mutual neglect.

In fact, many clients view these providers’ general disregard for takedown and enforcement requests as a (if not the) selling point. Promotional materials from BPH providers often describe their services as “bulletproof” or advertise “Offshore DMCA Ignored Hosting” in a nod to the U.S. Digital Millennium Copyright Act (DMCA), which prohibits the distribution of pirated media. By branding themselves as anti-DMCA, these providers are signaling that pirated or illegal content is welcome on their networks.



HOW BPHS GET ONLINE

The idea of a bulletproof host is simple enough, but identifying which IP blocks exhibit bulletproof behavior and maintaining a real-time list of the Autonomous Systems (AS) they belong to and shift between is a complex challenge rooted in how the internet itself is managed at scale.

At their core, an AS is simply a collection of IP routing prefixes (each set of prefixes may also be individually referred to as a 'block' or 'range') under the control of a singular entity. Autonomous System Numbers (ASNs) are used to identify those entities, and are issued by the [Internet Assigned Numbers Authority \(IANA\)](#) (a function of the [Internet Corporation for Assigned Names and Numbers, or ICANN](#)), down to the [Regional Internet Registries \(RIRs\)](#) and Local Internet Registries (LIRs).

Once registered, an AS operator is allowed to lease IP address blocks and establish routing relationships that connect their networks to the global internet. BPH operators often exploit this process by acquiring ASNs—a step that empowers them to control traffic flow, advertise entire IP ranges for use, and sustain operations even when elements or sections of their infrastructure for a given campaign are targeted by takedown efforts.

As most bulletproof hosts operate their own ASNs directly, this gives them full control over their infrastructure. Smaller operators, however, may rent IP space from either legitimate hosting providers or from other BPHs, resulting in a complex web of dependencies that only serves to further obscure true ownership and complicates enforcement.

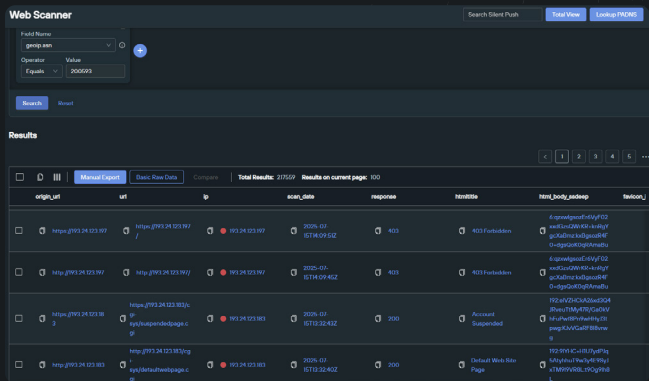
This is where Silent Push's change metrics make a powerful difference. Understanding how bulletproof hosts acquire and use ASNs is a critical part of our analysis, and understanding the movement behind it, even more so. Pairing these two together gives defenders unprecedented insight into the support infrastructure for malicious networks, and underscores how the same systems keeping legitimate networks online can inadvertently make malicious ones nearly impossible to shut down.

PUTTING ASN INTELLIGENCE INTO PRACTICE

Our analysts continuously monitor a network of over 200 ASNs linked to BPH activity, capturing the observable IP and domain footprint across each range to surface emerging threats. This process is illustrated below using Silent Push's [Web Scanner \(now Web Search\)](#) and Advanced [Domain Search](#) tools to investigate ASN 200593, a known BPH operating under the alias "Prospero."

Web Scanner ASN filter search query link

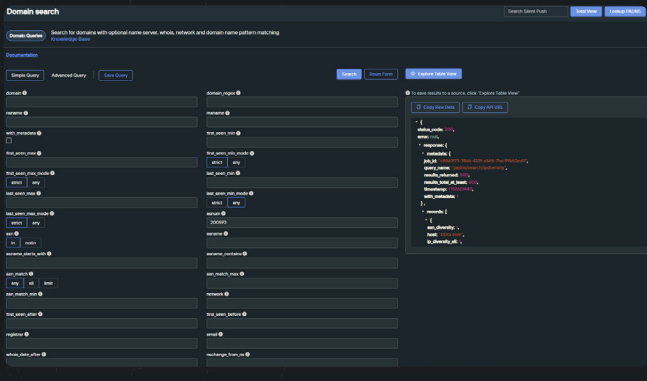
- datasource = ["webscan"] AND geoip.asn = 200593



Silent Push Web Scanner ASN search results

Advanced domain search query link

- ASN = 200593



Silent Push Advanced Domain search results, simply click "Explore Table View" from here to open a table of the results

Both tools act as a springboard for deeper analysis, providing analysts with flexible filters to drill further into specific types of infrastructure. Additional details to filter through and examine ASN results are described throughout this report.

THE SILENT PUSH PROCESS FOR IDENTIFYING BPHS

Our analysts follow a multi-stage review process when evaluating potential bulletproof hosts, which includes:

TRACKING INFRASTRUCTURE SHIFTS ACROSS ASNS AND HOSTING PROVIDERS

We meticulously curate a series of extensive **IOFA™** feeds for our enterprise customers to detect the early signs of threat actors relocating their infrastructure. Once identified, analysts investigate these new networks to confirm signs of emerging bulletproof hosting activity, often spotting suspicious hosts well before they appear on the radar of other vendors or in public reporting.

ANALYZING IP DENSITY AND PEERING LIMITATIONS AMONG BPHS

BPHs tend to control relatively few IP addresses, largely because of the difficulties inherent to renting and retaining these IP blocks. Providers often reclaim IPs the moment they're linked to abuse or illicit activity. These limitations are compounded by persistent "IP Peering" challenges that emerge when connected to illegal activity as upstream network operators block or refuse routes from suspected BPH ASNs. While not a conclusive factor by itself, IP density is nevertheless a reliable metric to look for when performing this type of analysis.

IDENTIFYING SUSPICIOUS WHOIS RECORDS

All ASNs are required to provide an email address for routing abuse complaints. We've found that ASNs associated with bulletproof hosting operations routinely list disposable or free email addresses (think Gmail or Proton Mail) in their WHOIS records. This is because they often lack a formal web presence or rely on leased infrastructure obtained through opaque or underground channels. Outliers to this trend exist, but the norm for legitimate enterprise networks is the use of domain-linked addresses for their abuse contacts. Anything else should be viewed with a reasonable degree of suspicion.

CATCHING CORPORATE REGISTRATION LOOPHOLES

Most BPH providers are headquartered in jurisdictions with limited government oversight of cybersecurity threats, like Russia, Ukraine, and China. Others incorporate in states or countries that allow remote business registration with minimal oversight, such as Wyoming, Delaware, Panama, and the Seychelles. It's not uncommon to find U.S. or U.K. business registrations tied to operators who have never set foot in those countries.

CORRELATING BPHS AND DGAS

Bulletproof hosts frequently service clients that lean on Domain Generation Algorithms (DGAs) to create and sustain their malicious infrastructure. The term DGA refers to automated tools that generate dozens to thousands of new domains. DGA-generated domains often resemble gibberish, with random strings of numbers, letters, or words strung together ([our investigation into CryptoChameleon](#) documents some illustrative examples). Even so, this isn't a hard-and-fast rule; absent clarity on underlying algorithms, even domains that appear unmistakably DGA-generated can only be classified on a best-guess basis. This limitation is particularly visible for domains registered in China, where numeric domains are common and frequently belong to legitimate websites.

SPAMHAUS: A GOLD STANDARD FOR CERTAIN THREATS

During the investigative process, our analysts will often cross-reference suspicious ASNs with [the Spamhaus "Don't Route or Peer" \(DROP\) list](#), a trusted industry resource for identifying networks linked to spam, malware, and botnet activity. While we've never encountered false positives when checking ASNs that Spamhaus has blocked, we have found these scores can veer conservative in their scope. Spamhaus heavily scores ASNs based on malware hosting and malware C2 visibility, but there doesn't appear to be a similar process for tracking and scoring phishing pages or malicious financial scams. This means that some ASNs that support more phishing than malware delivery, or various types of financial scams, are sometimes scored lower by Spamhaus than might be expected.

In short, Silent Push regards Spamhaus as a gold standard for initial insights into several types of threats, but not as a complete solution.

MAPPING ACTIVE INFRASTRUCTURE WITHIN BPH NETWORKS

Silent Push actively tracks more than 80 Bulletproof Hosting (BPH) providers and the nearly one million individual IP addresses under their control. Fewer than half of these IPs host active websites; the majority instead support command-and-control (C2) servers or illicit proxy and VPN services-both of which typically operate without any public-facing content or domain mappings.

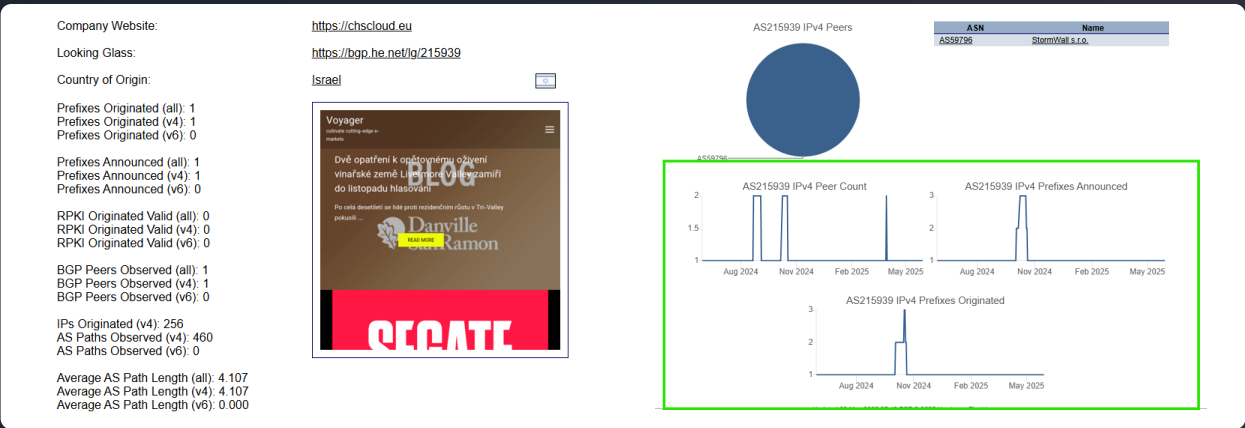
ASNs with small or unstable IP allocations are another common pattern among bulletproof networks. A good example of which is ASN 215939, which uses the abuse email “abuse@chsccloud[.]eu” within its WHOIS records. As of the time this report was created, our team had observed 48 active IPs on this network in the last 30 days.

ASN Information		WHOIS RDAP Data	
Name	Value	Name	Value
ASN	215939	Copyright Notice	-
ASN Size	-	Description	/I"/I
AS Name	MORNINGSTARS-AS_IL	Handle	ACRO65529-RIPE
Average Density	11.5	Email	abuse@chsccloud.eu
Density Max	93	Name	Abuse contact role object
Active IPs	53	Phone Number	-
Active Subnets	1	WHOIS Server	-
		URL	-
		Handle	VSIB6-RIPE
		Handle	CHSCLOUD-MINT
		Handle	MORNINGSTARS-MINT
		Handle	ORG-VS354-RIPE
		Handle	RIPE-NCC-END-MINT
		Handle	VSIB6-RIPE
		Expiration Date	-
		Last Changed Date	2025-06-21T17:41:43+00:00
		Registration Date	2023-11-27T08:11:10+00:00
		URL	https://rdap.db.ripe.net/autnum/215939
		Whois Server	whois.ripe.net

ASN Takedown Reputation	
Name	Value
ASN Allocation Age	549
ASN Allocation Date	20231127
ASN Takedown Reputation	0
IPs Active	48
IPs in ASN	0
IPs with URLs listed	1
Number of URLs listed	2
Lifetime Avg	7
Lifetime Max	7
Lifetime Total	14

Total View for ASN 215939 [Silent Push](#)

Further reviewing ASN 215939 and data from [Hurricane Electric’s BGP lookup tool](#) confirms this ASN has experienced sporadic peering. The ASN is sometimes online and sometimes offline, with only one active peer via ASN 59796 (StormWall s.r.o).



ASN report for AS215939

You are viewing the database entry for AS215939 (CHSCLOUD-AS).

Database Entry

AS number:	AS215939
AS name:	CHSCLOUD-AS
Country:	RU
Total IPs observed 🕒:	🔄 Loading
Online malware site 🕒:	🔄 Loading
Offline malware site 🕒:	🔄 Loading
Oldest active malware site 🕒:	🔄 Loading
Newest active malware site 🕒:	🔄 Loading
Average takedown time 🕒:	🔄 Loading
First seen:	🔄 Loading
Last seen:	🔄 Loading
Data export:	URLhaus ASN feed

URLhaus report on ASN 215939

If we look up this same [ASN 215939](#) within the [Spamhaus data on URLhaus](#), the data shows 0 IPs and essentially no data associated with the ASN. This is something we have consistently observed on URLhaus for some of the smaller ASNs we are currently classifying as BPH, based on the content hosted there and their policies regarding malicious hosts (or lack thereof).

Within Silent Push, we can also search for content hosted on ASN 215939 with a simple Web Scanner query. The results heavily feature various financial, pig-butcher investment, and cryptocurrency scams among them, which yielded about 2,700 results in total at the time of writing this report.

Web Scanner ASN and domain filter search query link

- datasource = ["webscan"] AND geoiip.asn = 215939 AND domain = "*"."

datasource = ["webscan"] AND geoiip.asn = 215939 AND domain = "*"."

Sort order: scan_date/asc

Reset

Results

Total Results: 1543Results on current page: 100

origin_url	scan_date	ip	geoiip.asn	htmltitle	html_body_sadseep	jarm	ssl.SHA256	path	
https://teminity.com	2025-05-28T00:48:04Z	62.60.227.87	215939	منصة مقارنة - تأمين شامل	192H9DmIjQokZbKtKg rCvHbTg7ZQFLLjMfB ue0hZU4ZwvdbA.Hj/L CgkZSILUgeuA	2ed2ad0002ed2ad00 042a42a0000000007 8d2ac0ce6e95bbc5b81 49e4872355	44:4B:A3:96:AF:66:00: 5E:50:F1:2B:9C:81:AB:0 E:4E:3C:AE:12:FO:6B:38 F174:EC:C3:E2:CF:DC: F5:37:12	/	Expand
http://teminity.com	2025-05-28T00:48:03Z	62.60.227.87	215939	منصة مقارنة - تأمين شامل	192H9DmIjQokZbKtKg rCvHbTg7ZQFLLjMfB ue0hZU4ZwvdbA.Hj/L CgkZSILUgeuA	2ed2ad0002ed2ad00 042a42a0000000007 8d2ac0ce6e95bbc5b81 49e4872355	44:4B:A3:96:AF:66:00: 5E:50:F1:2B:9C:81:AB:0 E:4E:3C:AE:12:FO:6B:38 F174:EC:C3:E2:CF:DC: F5:37:12	/	Expand
http://syertik.com	2025-05-28T00:42:07Z	62.60.227.86	215939	منصة مقارنة - تأمين شامل	192H9DmIjQokZbKtKg Tl9HbDM9tzuFg7xzDr Bue0hZU4ZwvdbA.Hj/L eoCzryq7KfYeuA	2ed2ad0002ed2ad00 042a42a0000000007 8d2ac0ce6e95bbc5b81 49e4872355	AF:CE:1D:CE:6B:B2:0C: 0B:28:F1:2B:1E:91:71:4D: A2:6C:E1:F8:E9:18:81:9E F8:95:8C:72:BA:5B:00: D1:6F	/	Expand
https://syertik.com	2025-05-28T00:42:07Z	62.60.227.86	215939	منصة مقارنة - تأمين شامل	192H9DmIjQokZbKtKg Tl9HbDM9tzuFg7xzDr Bue0hZU4ZwvdbA.Hj/L eoCzryq7KfYeuA	2ed2ad0002ed2ad00 042a42a0000000007 8d2ac0ce6e95bbc5b81 49e4872355	AF:CE:1D:CE:6B:B2:0C: 0B:28:F1:2B:1E:91:71:4D: A2:6C:E1:F8:E9:18:81:9E F8:95:8C:72:BA:5B:00: D1:6F	/	Expand
https://mrkabel.com	2025-05-27T19:24:27Z	62.60.227.85	215939	منصة مقارنة - تأمين شامل	192H9DmIjQokZbKtK4 fGfHb/mztV6fG/KHrB ue0hZU4ZwvdbA.Hj/L CoAtVvg/koeuA	2ed2ad0002ed2ad00 042a42a0000000007 8d2ac0ce6e95bbc5b81 49e4872355	29:28:61:0E:66:B8:8D:7 0:4D:B4:CA:F8:6A:CD: 0F:56:89:28:11:05:CE:0 A:5D:51:47:82:36:BC:EE 72:43:64	/	Expand
http://mrkabel.com	2025-05-	62.60.227.85	215939	منصة مقارنة - تأمين شامل	192H9DmIjQokZbKtK4 fGfHb/mztV6fG/KHrB	2ed2ad0002ed2ad00 042a42a0000000007	29:28:61:0E:66:B8:8D:7 0:4D:B4:CA:F8:6A:CD: 0F:56:89:28:11:05:CE:0	/	Expand

ASN and Domain filter Web Scanner search query results

SPOTTING SELF-DECLARED BPHS

Providers that openly label their services as “bulletproof” are treated as such initially, then vetted against our other methods and data sources to confirm those claims. We find that forums frequented by threat actors are where most of these claims first surface; forums like **BlackHatWorld** and **LowEndTalk** feature candid exchanges on everything from [the merits of different takedown-resistant hosts to the jurisdictions that are most tolerant of illicit hosting operations](#). The firsthand accounts shared by current and would-be BPH customers are just some of the many ways our analysts discover new providers before their infrastructure appears in public resources.

Our team has compiled a list of hosts whose own marketing confirms their bulletproof status, particularly when the marketing is less direct and references terms such as “offshore” or “DMCA-ignored,” as these claims often lead to indifference on the operators’ end when it comes to takedown laws or abuse reports:

AlexHost

AlexHost (alexhost[.]com) has been operating since 2008 and is based in Moldova. It controls [ASN 200019](#) (under the name “LEBEDEV-A-E”) with nearly 10,000 active IPs.

Domains mapped to this ASN can be found with this simple domain regex query:

Domain search with ASN filter

- domain_regex: ^(\xn--|)[^.]*(\xn--|)[a-z]{1,}\$
- asnum: 200019

The screenshot shows the 'Domain search' interface of Silent Push. The search query is defined by two filters: 'domain_regex: ^(\xn--|)[^.]*(\xn--|)[a-z]{1,}\$' and 'asnum: 200019'. The interface includes a 'Search' button and a 'Reset Form' button. On the right, there is a 'Total View' button and a 'Lookup PADNS' button. Below the search form, there is a 'Documentation' section with links to 'Simple Query', 'Advanced Query', and 'Save Query'. The search results are displayed in a table view, showing columns for 'domain', 'first_seen_min', 'first_seen_max', 'last_seen_min', 'last_seen_max', 'asnum', 'asname', 'asn_match', 'asn_match_min', 'first_seen_after', 'registrar', and 'whois_date_after'. The results table is currently empty. On the right side of the interface, there is a 'To save results to a source, click "Explore Table View"' button. Below this button, there is a 'Copy Raw Data' button and a 'Copy API URL' button. The 'Copy Raw Data' button is highlighted, and the raw data is displayed in a JSON format. The JSON data shows a successful search result for the domain 'alexhost.com' with a status code of 200, no error, and a response containing metadata and records. The metadata includes the job ID, query name, results returned, results total at least, and timestamp. The records array contains one record for the domain 'alexhost.com' with the host '00019.com' and the ip_diversity '1'.

```
{
  "status_code": 200,
  "error": null,
  "response": {
    "metadata": {
      "job_id": "27b5626c-dbd0-487f-91e3-424e92c7239b",
      "query_name": "padns/search/ipdiversity",
      "results_returned": 100,
      "results_total_at_least": 200,
      "timestamp": 1752601670,
      "with_metadata": 1
    },
    "records": [
      {
        "asn_diversity": 1,
        "host": "00019.com",
        "ip_diversity": 1
      }
    ]
  }
}
```

Silent Push Domain search with ASN filter results

Web Scanner ASN 200019 search query link

- datasource = ["webscan"] AND geoip.asn = 200019 AND domain = "*"."

Web Scanner Search Silent Push Total View Lookup PADNS

Field Name: geoip.asn Operator: Equals Value: 200019 AND Field Name: domain Operator: Contains Value: *

Results Manual Export Basic Raw Data Compare Total Results: 975734 Results on current page: 100

origin_url	url	ip	scan_date	response	htmltitle	html_body_sdeap	favicon_icons	header.server	sslissuer.organization
http://mangokurs.com	https://lovekurs.com	91.208.206.177	2025-07-15T17:42:34Z	200	Сила курсов 200 000 - Онлайн курсы, вебинары скачать бесплатно	61447e2WyN+1UfH4+UpqzMelvIOLb79D3grfzWywIUbUpz8vIOLbB7lj		Tengine	Let's Encrypt
https://mae-casino-malaysia.com	https://mae-casino-malaysia.com/	37.221.65.150	2025-07-15T17:30:12Z	200	Site is undergoing maintenance	96Z1+8nOQ36VVLb9N0kNUK1q7HoOxSUZZdGYCq8GRrGYExmIVXxleOxQ3DNBZ9rHIQa6VxLb8GUygtZdoGRWuxgedBd		nginx/1.28.0	Let's Encrypt
http://liverpooltravel.com	http://liverpooltravel.com/	176.123.5.236	2025-07-15T17:20:03Z	200	Liverpooltravel.com	384Ldc5J4Qn8+9Br7Qq1319DIXMhO9rdQ9yO93vG9U8OY3pNOuKTOu3GQ5uH1qJ4Q8+95Aa6d6BI		nginx	Let's Encrypt
https://liverpooltravel.com	https://liverpooltravel.com/	176.123.5.236	2025-07-15T17:19:56Z	200	Liverpooltravel.com	384Ldc5J4Qn8+9Br7Qq1319DIXMhO9rdQ9yO93vG9U8OY3pNOuKTOu3GQ5uH1qJ4Q8+95Aa6d6BI		nginx	Let's Encrypt
https://support-imaps.app	https://support-imaps.app/	91.208.197.78	2025-07-15T17:18:45Z	404	support-imaps.app	3072-wIGDv974/c7BMrtpa8lqk66w3veOALu1BbMy8Ck5u0x2ec7BUUp66LurReAE		Apache	Let's Encrypt

Silent Push Web Scanner ASN search results

Across the AlexHost website, there are numerous examples where it openly brags about providing "Offshore DMCA Ignored Hosting," including on the page alexhost[.]com/DMCA as seen below.

AlexHost Hosting VPS Dedicated Server BEST GPU Hosting NEW Services Company Contacts

Offshore DMCA Ignored Hosting

Experience enhanced privacy, freedom, and uninterrupted uptime without the threat of arbitrary takedowns or DMCA claims. Hosting on servers beyond restrictive jurisdictions grants you greater control, security, and operational independence.

4.3 [Read our 112 reviews](#)

Source: alexhost[.]com/DMCA

On AlexHost and similar BPHs, we can search for phrases like “free movies” using the Silent Push Web Scanner with an ASN filter and immediately find countless websites that openly flout copyright laws.

Web Scanner ASN search with “free movies” HTML filter query link

- datasource = [“webscan”] AND geoip.asn = 200019 AND htmltitle = “*free movies*”

origin_url	scan_date	ip	geoip.asn	htmltitle	html_body_ssdeep	jarm
http://movie2k.let	2025-06-18T07:25:00Z	85.239.34.205	200019	Watch Free Movies Online	1536:JxUCJURDQOpIEL50E8f+TgdybSI0IXu/K4eL0E8PJLqj+70aM50L+TgLoaZLOE8PJL	3fd3fd0003fd3fd21c4d42d000000bdfc58c9e4a43438cf60ee440385763
http://filmeserialeonline.live	2025-06-17T16:36:08Z	176.123.7.251	200019	filmeserialeonline Watch Free Movies online	384:d29QPvPMPSv/YH9PC3H8eIOTL9nvbMatv/kgPvq3:d29OnPMPS/YH9PC3H8eIOTL9nvbDPvs	29d29d00029d29d0c042d4d000000209a3b9f6e99461c5923779b77cf08b
https://freetubespot.one	2025-06-10T13:43:50Z	37.221.67.157	200019	Freetubespot - Watch Free Movies & TV Shows Full HD	768:fyKGU07zcVURYbunkeNGVuhJlfe3Fy//wwwPMVjyrcAPy//lvePMFjyLYNGZdayfY8xDVuhJLZepwgoRTSZT8ECT	29d29d00029d29d0c043d4d0000004d46afe8cfbe9e42e031eb5c55d6787
https://85.239.34.205	2025-06-30T03:25:14Z	85.239.34.205	200019	Watch Free Movies Online	1536:-v4WKNDM4kMrKTyb/0RfKwstHghuuf0E8PJW/Ukx4R2TwzHqJ0E8PJW	3fd3fd0003fd3fd21c4d42d000000bdfc58c9e4a43438cf60ee440385763
https://91.229.239.140	2025-05-29T23:17:05Z	91.229.239.140	200019	WMOVIES - Your Destination for Free Movies & TV Shows	768:ajOCNpC1+hUK72PiQ80GeloQpZehq/AMORUajOCNpCHV72zG7TMOA	15d3fd1ed29d29d00042d43d0000009ac616233e4398bee334bafe62a34e01

Silent Push Web Scanner ASN search with “free movies” filter

According to Hurricane Electric, [ASN 200019](#) is currently peered with 23 other ASNs. For context, an ASN from an enterprise service like [Cloudflare](#) has over 1,800 peers. In a sample 8-day window, our team discovered over 400 malicious domains pointing to AlexHost IPs based on fingerprints used to track a number of unrelated threat groups.

ABOLLY WEB SOLUTIONS

One bulletproof host, “Abolly Web Solutions” (abollyhost[.]com), maps its client websites with Name Server (NS) records, which can be seen with the query below. As a helpful tip for defenders, NS records are particularly useful for threat hunting even outside of mapping BPH infrastructure, and we encourage those reading this report to incorporate them into their own investigations.

[Reverse NS lookup query link](#)

■ *.abollyhost.net

Explore

Search Silent Push

Total View

Lookup PADS

Explore

Basic Raw Data

< Previous

Monitor

*.abollyhost.net

NS

Density:

Total Results: 9993 Results on current page: 100

Clear Filters

Query

Answer

First Seen

Last Seen

Name Server Hash

TTL

legogigbedu.com

dns2.abollyhost.net

2021-08-23 16:08:40

2025-07-15 17:48:18

e0289c41b4c6...

86400

legogigbedu.com

dns1.abollyhost.net

2021-08-23 16:08:40

2025-07-15 17:48:18

e0289c41b4c6...

86400

zmovies.ng

dns1.abollyhost.net

2024-11-10 11:53:05

2025-07-15 17:43:54

e0289c41b4c6...

86400

zmovies.ng

dns2.abollyhost.net

2024-11-10 11:53:05

2025-07-15 17:43:54

e0289c41b4c6...

86400

elexdonhost.com.ng

dns2.abollyhost.net

2023-03-12 19:05:26

2025-07-15 17:43:14

e0289c41b4c6...

86400

elexdonhost.com.ng

dns1.abollyhost.net

2023-03-12 19:05:26

2025-07-15 17:43:14

e0289c41b4c6...

86400

unitree-services.xyz

dns1.abollyhost.net

2025-05-17 16:52:05

2025-07-15 17:39:19

e0289c41b4c6...

86400

unitree-services.xyz

dns2.abollyhost.net

2025-05-17 16:52:05

2025-07-15 17:39:19

e0289c41b4c6...

86400

trustremedy.com.ng

dns1.abollyhost.net

2022-05-03 21:39:02

2025-07-15 17:36:56

e0289c41b4c6...

86400

trustremedy.com.ng

dns2.abollyhost.net

2022-05-03 21:39:02

2025-07-15 17:36:56

e0289c41b4c6...

86400

charlotthomesandprope
rties.org

dns1.abollyhost.net

2025-05-22 21:19:27

2025-07-15 17:30:50

e0289c41b4c6...

86400

charlotthomesandprope
rties.org

dns2.abollyhost.net

2025-05-22 21:19:27

2025-07-15 17:30:50

e0289c41b4c6...

86400

mixo.live

dns1.abollyhost.net

2025-06-07 13:40:29

2025-07-15 17:29:39

e0289c41b4c6...

86400

mixo.live

dns2.abollyhost.net

2025-06-07 13:40:29

2025-07-15 17:29:39

e0289c41b4c6...

86400

getcala.app

dns1.abollyhost.net

2025-06-06 11:26:27

2025-07-15 17:27:22

e0289c41b4c6...

86400

getcala.app

dns2.abollyhost.net

2025-06-06 11:26:27

2025-07-15 17:27:22

e0289c41b4c6...

86400

www.teemasdigital.co
m

dns2.abollyhost.net

2025-04-29 00:30:33

2025-07-15 17:23:11

e0289c41b4c6...

86400

www.teemasdigital.co
m

dns1.abollyhost.net

2025-04-29 00:30:33

2025-07-15 17:23:11

e0289c41b4c6...

86400

Silent Push Reverse Name Server records lookup search results

Abolly Web Solutions.'s Post

Abolly Web Solutions.
September 6, 2024 · 🌐

100% anonymous and DMCA ignored Offshore server is available to be configured according to your requirements with 100% uptime guaranteed, what are you waiting for? Contact us today on <https://abollyhost.com/anonymous-hosting>



Abolly Web Solutions.
Web Designer

WhatsApp

39

Abolly Host [boasts on its Facebook page](#) that it is a “100% anonymous and DMCA ignored Offshore server,” and its [website claims](#) it is “DMCA Offshored Ignored,” in providing “Bulletproof Anonymous Hosting.”

Source: facebook[.]com/abollyhost/posts/pfbid0ETxLB3LUeThyKs q7Ro1vcYhc5X974rutc25HGefc2FTVX6RcMHe2vUZptkdYN41l

Similar to many other BPHs, Abolly Host has a small network footprint. Its two NS domains are mapped to [a single IP on Hetzner Networks 95.216.25\[.\]188](#), ([Record Two](#), same data)—an enterprise host in Germany—and has been since 2023.

Bulletproof Hosting Reseller

We have received great journey serving far off consumers in Africa and other regions. We can procure, deploy and utterly guide any quantities of tools in our Tier 2 to licensed Tier 3 statistics facilities in Russia, Germany, USA and UK. We can provide very cheaper & best Bulletproof Anonymous Hosting in replace of DMCA Offshored Ignored with 100% Uptime Guaranteed

	Basic	Standard	Premium	Giant
	<div>₦</div> 42,000/month	<div>₦</div> 65,000/month	<div>₦</div> 90,000/month	<div>₦</div> 150,000/month
Disk Space	15 GB SSD	25 GB SSD	50 GB SSD	100 GB SSD
Bandwidth	15000 GB	Unlimited	Unlimited	Unlimited

Source: [abollyhost\[.\]com/anon-directadmin-reseller/](https://abollyhost[.]com/anon-directadmin-reseller/)

PHANES NETWORKS

Phanes Networks ([phanes-networks\[.\]com](https://phanes-networks[.]com), [phanes\[.\]cloud](https://phanes[.]cloud)) was founded in 2017 and is legally based in the Netherlands.

Phanes Network controls ASN 49042 (which [Spamhaus](#) recommends blocking) and reports a 4-day abuse response time. A 4-day abuse response time may not seem long, but it provides ample time for threat actors launching campaigns by the minute, who are ready to hop onto different accounts as soon as any is taken down.

On its [“high-privacy-offshore-VPS” hosting page](#), Phanes brazenly states that there’s, “No need to worry about DMCA Complaints now,” while another page explicitly lists its services as “bulletproof”:

Phanes Cloud

Select Your Perfect Plan

No need to worry about DMCA Complaints now!

Categories

- Compute - Basic
- Compute - Cloud Servers
- Compute - Resource Packs
- Shared Hosting - cPanel

Offshore 1GB
€20,00 EUR
Monthly

Offshore 2GB
€30,00 EUR
Monthly

Offshore 4GB
€50,00 EUR
Monthly

Source: [my\[.\]phanes\[.\]cloud/index.php?rp=%2Fstore%2Fhigh-privacy-offshore-vps](https://my[.]phanes[.]cloud/index.php?rp=%2Fstore%2Fhigh-privacy-offshore-vps)

Phanes Cloud

Bulletproof VPS

Categories

- Compute - Basic
- Compute - Cloud Servers
- Compute - Resource Packs
- Shared Hosting - cPanel
- Reseller Hosting
- Bare Metal Servers
- Windows Hosting
- SSL Certificates

Linuxoid 8GB
8GB RAM
2 Cores
200GB SSD Storage
1 IPv4
200Mbit/s Unmetered bandwidth
€34,99EUR
Monthly
Order Now

Linuxoid 16GB
16GB RAM
6 Cores
400GB SSD Storage
1 IPv4
400Mbit/s Unmetered bandwidth
€69,99EUR
Monthly
Order Now

Linuxoid 32GB
32GB RAM
8 Cores
800GB SSD Storage
1 IPv4
600Mbit/s Unmetered bandwidth
€109,99EUR
Monthly
Order Now

Linuxoid 64GB
64GB RAM
10 Cores
1600GB SSD Storage
1 IPv4
800Mbit/s Unmetered bandwidth
€199,99EUR
Monthly
Order Now

Source: [my\[.\]phanes\[.\]cloud/index.php?rp=/store/bulletproof-vps](https://my[.]phanes[.]cloud/index.php?rp=/store/bulletproof-vps)

On ASN 49042, a significant amount of infrastructure is associated with malicious “Download XYZ App” campaigns targeting a wide range of users. Most of these domains serve different content to different visitors, so some may see benign content, while others may see prompts to download.

Once again, building a query to investigate some of these suspicious campaigns is simple to perform within the Silent Push Web Scanner, as seen in the example below.

Web Scanner ASN 49042 search with “download” HTML title filter query link

■ datasource = [“webscan”] AND geoip.asn = 49042 AND htmltitle = “*download*”

origin_url	scan_date	ip	geoip.asn	htmltitle	html_body_ssdeep	jarm
http://helloneighbor2-free.net	2025-06-25T13:23:40Z	45.148.120.37	49042	Hello Neighbor 2 for Free ↓ Download	384:ulBnJAUZzG/svmMqLWvh2WLNrL8vOvi	21d19d00021d21d21c1d19d21d21d188f9fde1e4d1b361b3e6ec49412d2
http://capcutclub.com	2025-06-25T12:57:43Z	45.148.120.37	49042	CapCut App ↓ Download CapCut for Windows 10/11 PC or Laptop for Free (Desktop Version)	384:nLYEnD+/VC4UeMk89eNYBBVNH2lw6wvP93DgoLFRIIZq8kB2eNIR2z3H2in6wxcLY+DGvC4Uc15Y3b2e9gOgS1eT2hx	21d19d00021d21d21c1d19d21d21d188f9fde1e4d1b361b3e6ec49412d2
http://procreatewin.com	2025-06-25T11:27:16Z	45.148.120.37	49042	Procreate for Windows ↓ Download Procreate App for Free for PC	768:LPWtIGutPDogTzRrW6tNNSlvnjdDj4woZrEDJL4GLPWtIGEPITzNW5tNNAjdDgtEB4G	21d19d00021d21d21c1d19d21d21d188f9fde1e4d1b361b3e6ec49412d2
http://capcut-win.com	2025-06-25T11:18:05Z	45.148.120.37	49042	CapCut for Windows ↓ Download CapCut App for Free: Install on Laptop & Desktop	768:8wQ26tWnlxTdXaKAAeJ/g1PqWBZUNHm1cVd:TO7WnlNdxFe6eJ4oWBZUvmlcVd	21d19d00021d21d21c1d19d21d21d188f9fde1e4d1b361b3e6ec49412d2
http://geforce-experience-free.com	2025-06-25T10:05:33Z	45.148.120.37	49042	GeForce Experience for Free ↓ Download GeForce Experience App for Windows 10/11/7 & Mac	768:*3jgbv3x3utQ9GloF+5TJERE8Lm81xC4mJfK1YxCOLTf5qPzb2dM+TPeAloXTJEhoxqfIKtYMOlnOe	21d19d00021d21d21c1d19d21d21d188f9fde1e4d1b361b3e6ec49412d2

Silent Push Web Scanner ASN search with “download” filter results

According to Hurricane Electric, [ASN 49042](#) has only one peering partner, AS62068, also known as SpectralP B.V. (spectraip[.]net), which is based in the Netherlands. Phanes explicitly confirmed this relationship via a [January 2025 announcement](#) stating that “as part of a strategic decision,” Phanes had “transferred its IT service operations, including dedicated servers, cloud VPS, and web hosting, to SpectralP B.V.”

SpectralP (AS62068) currently shows no signs of network abuse and has unannounced IP ranges. We will monitor this ASN closely to detect and address any malicious activities originating from their network.

SHINJIRU

Shinjiru (shinjiru[.]com) - [ASN 45839](#) - operates out of Malaysia and has been in business since 2000. According to Hurricane Electric, [ASN 45839](#) is peered by 19 different organizations/ASNs.

Shinjiru is currently [not recommended for a block by URLHaus](#), but it has a documented 12-day abuse desk response time, which is very poor. This timeframe essentially guarantees that a threat actor's campaign will have plenty of time to run its course even after being reported. This company also recently noted that it ignores all DMCA complaints, explaining [on a previous version of its FAQ page](#) that it, **"operate[s] under the DMCA ignored policy across all of our hosting services and locations.** This means that we won't take down content based on copyright infringement complaints."

Frequently Asked Questions (FAQ)

What Are the Rules and Policies for DMCA-Ignored Offshore Hosting at Shinjiru?

We operate under the DMCA ignored policy across all of our hosting services and locations. This means that we won't take down content based on copyright infringement complaints. However, please be aware that we are still required to comply with local legal authorities and domain registrar/registry suspension notices. If your content is reported for violating these regulations, our Trust and Safety team will be in contact with you to remove the content.

Additionally, our basic conditions prohibit activities such as spamhaus blacklisting and phishing. Any reports of these activities will result in removal of the reported content. You can review our full Acceptable Use Policy (AUP) for more details at the following link: <https://www.shinjiru.com/acceptable-use-policy-aup/>

Here are our basic rules:

- (1) No spamhaus blacklisting
- (2) No network interruptions - we cannot allow your activities to interrupt our network or affect our customers' business
- (3) No phishing or scamming
- (4) Compliance with any complaints from local authorities.

How does Shinjiru handle fake complaints or takedown requests?

What happens if I am not satisfied with my hosting plan?

Why should I choose Shinjiru's Budget Offshore Hosting over other providers?

Does the hosting include protection from DDoS attacks?

Can I host multiple websites under the Budget Linux Hosting Plans?

What payment methods are anonymous for Budget Offshore Hosting?

Are SSL certificates included in ALL Shared Hosting plans?

Source: [web\[.\]archive\[.\]org/web/20250502063104/https://www\[.\]shinjiru\[.\]com/offshore-web-hosting/budget-offshore-hosting/](web[.]archive[.]org/web/20250502063104/https://www[.]shinjiru[.]com/offshore-web-hosting/budget-offshore-hosting/)

Shinjiru also currently has pages on its website, such as a ["Bitcoin Hosting"](#) page, that describes not requiring personal details, including bank or credit card information. While on the surface this is to support privacy-conscious individuals, it also helps threat actors. As an interesting note: our team has never found a BPH that didn't accept cryptocurrency as a form of payment.

It's worth noting that Shinjiru has updated its website since we first took that snapshot. The new version has more ambiguous policies regarding DMCA abuse, despite being a relatively old host. It claims to now take action against a wide range of threats and malicious use cases, as defined in its [Acceptable Use Policy](#).

Overview

We respect your privacy, we never collect or mishandle customer information and we accept BitCoin! Shinjiru Offshore is a perfect anonymous hosting option for you. Our system allows you to stay anonymous and protect your identity by using BitCoin payments. BitCoin is all the rage now, since it is not controlled by any central authority or bank, so you are not tied up to any government or jurisdiction - no one will know who you are!

- BitCoin accepted
- No bank or card details required
- Ensured Privacy
- Uptime guarantee
- No personal details required
- 24/7 Live Support

Source: [shinjiru\[.\]com/bitcoin-hosting/](shinjiru[.]com/bitcoin-hosting/)

Within this updated document, Shinjiru also alleges it reserves the right to take immediate action, including banning accounts without notice, for certain violations. However, typically, clients have 10 days to respond to an abuse complaint before this happens. When a host has a policy like this with an extended (10 day) grace period, the average domain takedown ends up taking nearly two weeks.

Our team reached out to Shinjiru customer support in late June 2025, where they explicitly said, “We operate under the DMCA ignored policy across all of our services and locations,” while explaining some violations it claims to still take action on. This is part of an outreach effort our team regularly undertakes, as it can simplify the attribution process.

Despite the claims made above, Shinjiru has [a corporate fact sheet](#) where it claims numerous industry partner recognitions from companies such as Microsoft, Intel, Google, cPanel, Comodo, and Thawte. This host even [sells bundled Microsoft 365 products](#), has a [partner page on the cPanel website](#), and may have other official partnerships in alignment with these claims.

Investigation & Cancellation of Services

Shinjiru reserves the right to disable service or terminate service and/or to remove content in order to investigate suspected violations of this AUP. Shinjiru at its best effort will notify any customers of any violation so that the customer can investigate the case and provide necessary explanation or solution. Failure to respond to email from our abuse department may result in the suspension or termination of services. In some critical cases, Shinjiru reserves the right to disable or terminate service without first given notice if the violation affects the entire operation. If the explanation or solution is accepted, customer is given a warning and/or incurs an abuse fees. If Shinjiru feels as though this first offense was a deliberate attempt then the account and all associated accounts will be closed without warning and without a refund. Shinjiru does not issue refunds for terminating service due to any of the causes specified above. Dedicated Server or Websites with unresolved Abuse or AUP matters which are not responded to within 10 days will be considered abandoned and will be deleted from the offending account.

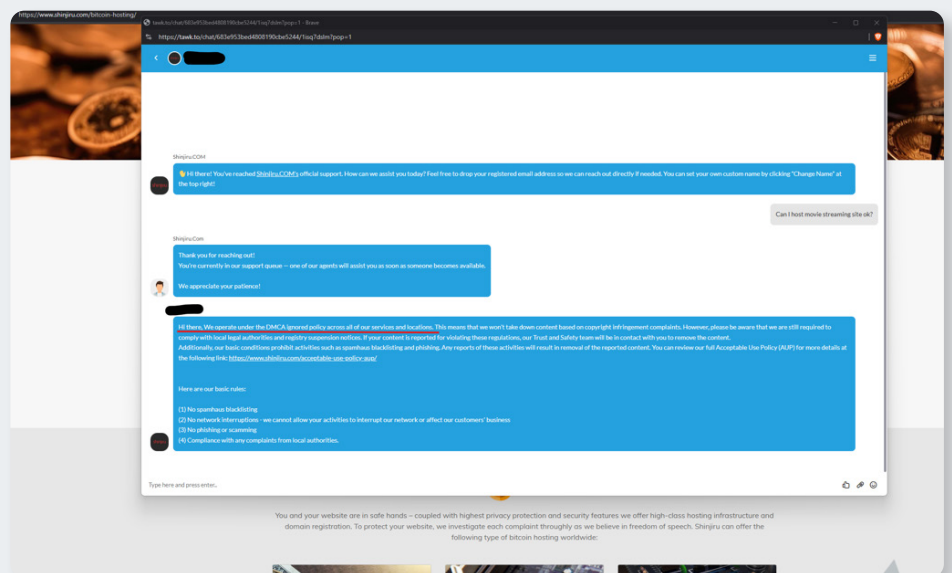
If your or your end users' actions have caused the Shinjiru mail servers or IP address ranges to be placed on blacklists and other mail filtering software systems used by companies on the internet, you will be assessed a USD100 abuse administrative charge and fees of USD100 per hour for employee time incurred to contact list holders, remove any blocks and protect our mail servers and IP ranges.

Shinjiru reserves the right to refuse service to anyone. Any material that, in our judgment, is illegal, of threats or violates our terms of service in any manner may be removed or suspended from our servers with or without notice.

For Resellers: We will suspend the site in question and will notify you to take action. If Customer's account has repetitive occurrence of this type, it may result in the immediate termination of Customer's account.

For Direct customers: Customer's services will be terminated with or without notice.

Source: [shinjiru\[.\]com/acceptable-use-policy-aup/](https://shinjiru[.]com/acceptable-use-policy-aup/)



Screenshot of a brief conversation with Shinjiru customer support

Recognition And Acknowledgments

- ICANN Certified Domain Registrar
- cPanel Certified Partner
- Microsoft Certified Partner
- Parallels Gold Partner
- INTEL Channel Partner
- Google Co-Marketing Partner
- COMODO SSL Reseller
- Thawte SSL Reseller
- Global SSL Reseller

Source: [shinjiru\[.\]com/company/about-us/](https://shinjiru[.]com/company/about-us/)

To further investigate the content currently hosted on Shinjiru, the Silent Push Web Scanner features an easy-to-use ASN filter that can be combined with all of the other filters available in our Web Scan data source.

Web Scanner ASN query with HTML title filter

- datasource = ["webscan"] AND geoip.asn = 45839 AND htmltitle = "*bank*"

Web Scanner Search Silent Push Total View Lookup PADS

Field Name: geoip.asn Operator: Equals Value: 45839 AND Field Name: htmltitle Operator: Contains Value: bank

Results Manual Export Basic Raw Data Compare Total Results: 1182 Results on current page: 100

origin_url	url	ip	scan_date	response	htmltitle	html_body_snippet	favicon_icons	header_server	sslissuer.organization
http://bankroll-app.com	https://bankroll-app.com/	111.90.156.115	2025-07-15T20:27:04Z	200	Bankroll	307295bVnkuYkAOKd74uB83EIL2L8cug5Rt		LiteSpeed	Let's Encrypt
http://swisscryptobank1.org	https://us.swisscryptobank1.com/	101.99.77.51	2025-07-15T19:56:33Z	200	Swiss Crypto Bank1	24n0eatIOUS6rNB5HYZS2NAJH0Hpp99Vvr		LiteSpeed	Let's Encrypt
http://republictrustbank.com	https://republictrustbank.com/	111.90.142.239	2025-07-15T19:46:09Z	200	Republic Trust Bank - Savings, Business Finance, Property Finance, Personal Loans	1536XIKJBVRcoxdW81VNGXkOZZK7Y7WVh		LiteSpeed	Let's Encrypt
http://leadunioninc.com	http://leadunioninc.com/	78.40.143.26	2025-07-15T18:41:29Z	200	Lead Union Inc - Dedicated to innovating, simplifying, and humanizing digital banking.	1536hGuRhuuZaJTXHJB8SBSEf77		LiteSpeed	
http://juntbank.com	https://juntbank.com/	78.40.143.12	2025-07-15T17:54:52Z	200	Home Mobile Banking, Credit Cards, Mortgages, Auto Loan	768d+kygVwqGGRXR		LiteSpeed	Let's Encrypt

Silent Push Web Scanner ASN search with HTML title filter results

Within these results, we can see plenty of suspect infrastructure, some of which directly impersonate real banks with phishing pages, and others that host investment scams.

https://commercebt.com/ebusiness/login.php

Commerce Bank & Trust

Commerce Bank & Trust Online Contact Us

Log in to Online Banking

To log in to your Online Banking account, enter your User ID and Password and click Log In.

User ID:

Password:

Start Page: ☐ Use as my default start page

[Forgot your user ID?](#) [Forgot your password?](#)

New to Online Banking?

- [Request for Login](#)

Welcome to Our Online Bank

This Online Banking provides access to deposit, loan, line of credit and investment accounts.

Don't have an account yet?

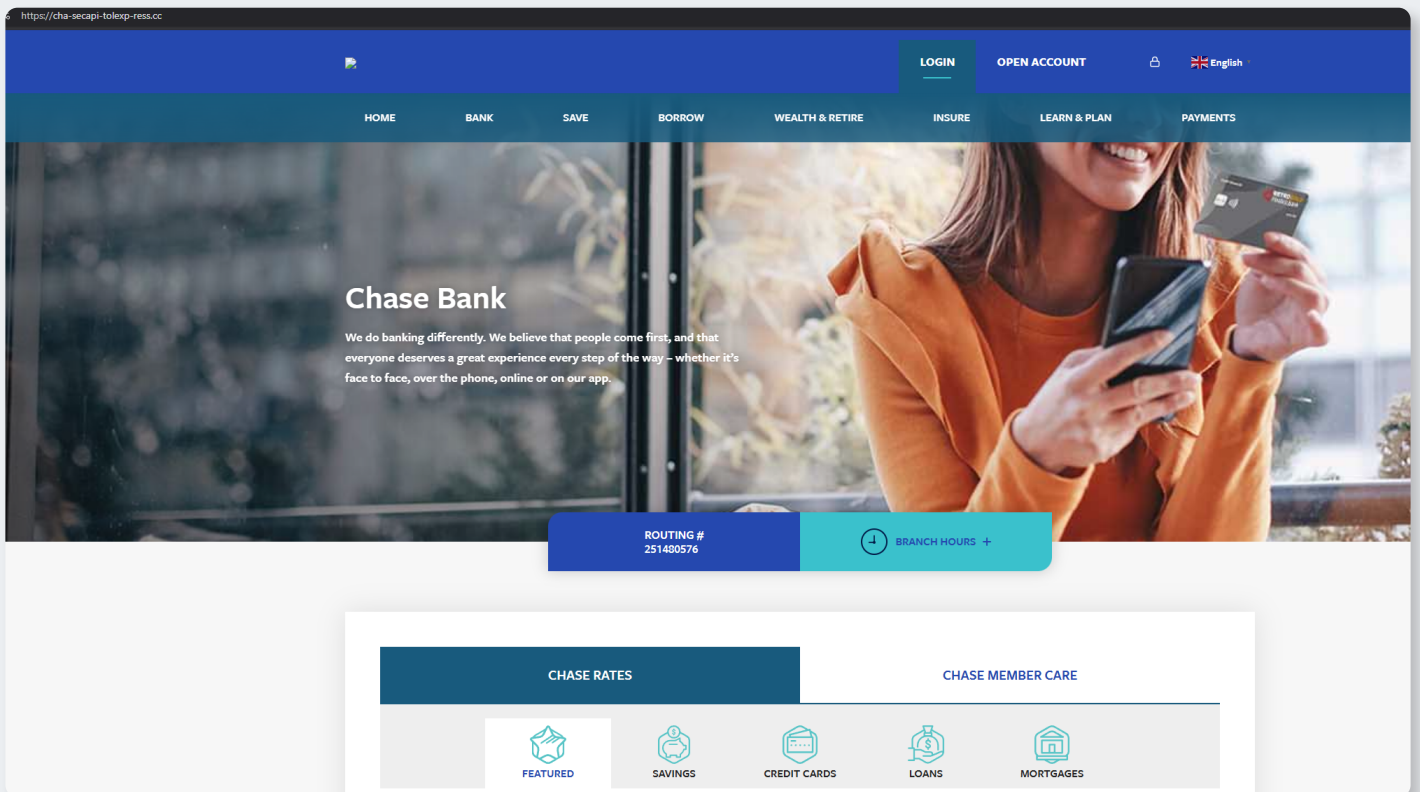
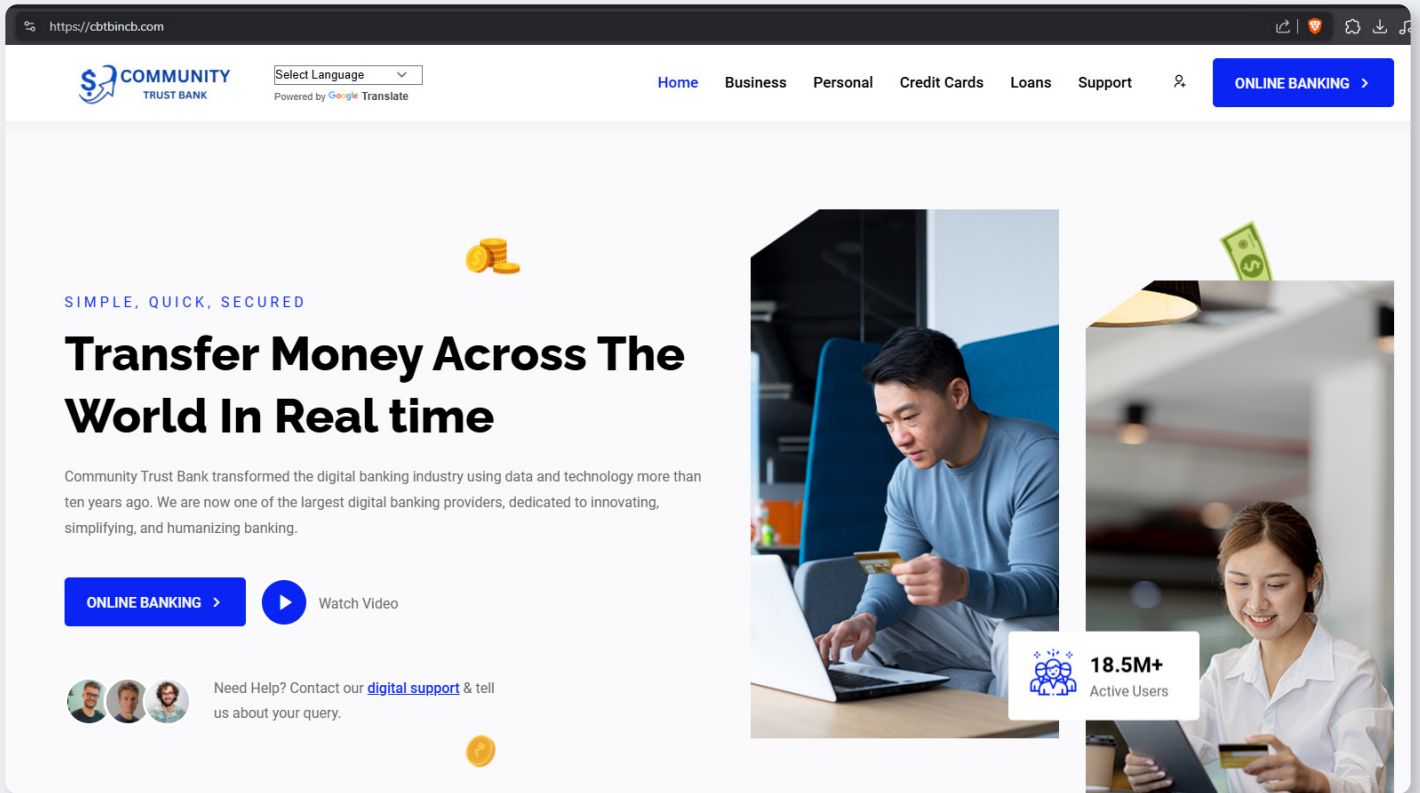
Join our league of happy customers today.

Commerce Bank & Trust Online Home

This site provides information about and access to financial services offered by Commerce Bank & Trust Online.

© 2025 Commerce Bank & Trust Online. All rights reserved.

Source: commercebt[.]com/ebusiness/login.php



As we would expect from a service that boasts about ignoring DMCA compliance, we can find numerous movie, TV, and sports streaming websites featuring stolen content using simple queries in our Web Scanner.

Web Scanner ASN query with "Movies" HTML title filter

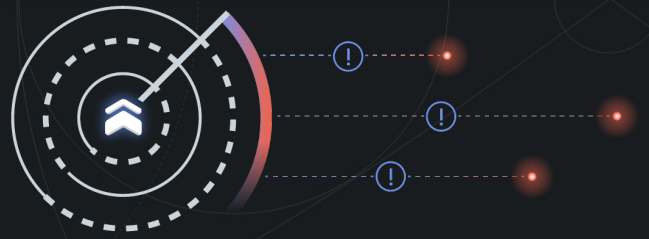
- `datasource = ["webscan"] AND geoip.asn = 45839 AND htmltitle = "*movies"`

[illegible]

Notably, Malaysia-based Shinjiru does have a small portion of clients who run legitimate businesses, personal websites, and host on its network. However, inadvertently or not, Shinjiru's policies and operational methods allow malicious clients and threat actors to continue operating with impunity across its network.

Due to the above, until Shinjiru starts to comply with DMCA abuse complaints, changes its 10-day grace period for abuse complaints, proactively hunts its own network for malicious infrastructure or begins to regularly cooperate with those who do, and improves its 12-day abuse response times as documented by Spamhaus/URLHaus, it will remain classified as a bulletproof host by our team. Until such time, organizations should keep on the alert for connections to their infrastructure and consider blocking those connections for their own protection.

ACTIONABLE QUERIES & RED FLAGS FOR DEFENDERS TO INVESTIGATE



AS NUMBER: 152194

- **AS Name:** CTGSERVERLIMITED-AS-AP
- **Red Flags:** Heavy DGA Usage, Spamhaus Blocklist
- **Domain:** ctgserver[.]com
- **ASN Details:** This ASN is heavily utilized by certain threat actors, primarily based in China. Spamhaus recommends blocking this ASN and documents on Abuse[.]ch that it has an average 24-day response time for abuse complaints.
- **DGA Details:** There is a massive backlog of content hosted on this ASN. Fortunately, the Silent Push Web Scanner empowers defenders with advanced query options. We can use these to exclusively surface sites with "live content" by using the "scan date" filter for specific time ranges, which can help to confirm the massive amount of DGA domains hosted there at any given point.

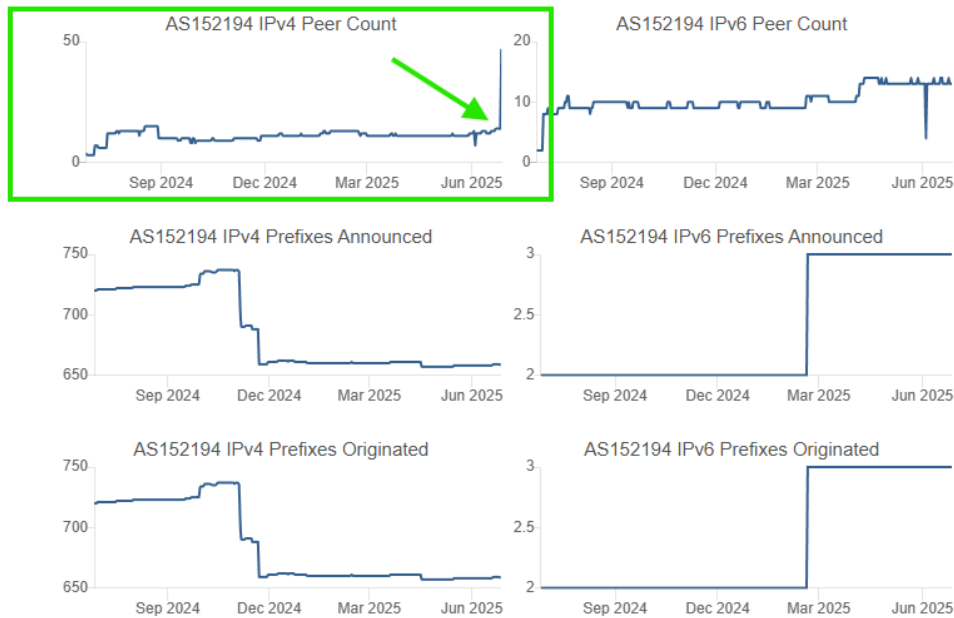
[Web Scanner ASN 152194 search with content filter to find DGA domains query link](#)

- `datasource = ["webscan"] AND geoip.asn = 152194 AND scan_date > "2025-02-01T22:40:15Z" AND htmltitle != "400 Bad Request" AND htmltitle != "404 Not Found" AND htmltitle != "域名未配置" AND htmltitle != "IIS Windows Server" AND htmltitle != "400 Invalid Hostname" AND htmltitle != "Login" AND htmltitle != "Error 409" AND htmltitle != "index" AND htmltitle != "Document" AND htmltitle != "Error 404 Not Found" AND htmltitle != "403 Forbidden" AND htmltitle != "Sorry, the website has been stopped" AND htmltitle != "后台管理系统" AND htmltitle != "没有找到站点" AND htmltitle != "最新域名" AND htmltitle != "Welcome" AND htmltitle != "Captcha Challenge" AND htmltitle != "*Welcome to*" AND htmltitle != "网络错误" AND domain = "*. *" AND domain != "*.cn*" AND htmltitle != "LVMH" AND htmltitle != "立信娱乐"`

<div> <div>Menu Quick Search</div> <div> <div>dataexport</div> <div>Threat Intelligence Management</div> <div>Web Data</div> <div>Web Scanner</div> <div>Live Scan</div> <div>WHOIS Data</div> <div>DNS Data</div> <div>Attack Surface Mapping</div> <div>Brand Impersonation</div> <div>Query History</div> <div>Monitors</div> <div>Advanced Query Builder</div> </div> </div>									
<div> <div>datasource = ["webscan"] AND geoip.asn = 152194 AND scan_date > "2025-02-01T22:40:15Z" AND htmltitle != "408 Bad Request" AND htmltitle != "404 Not Found" AND htmltitle != "域名未配置" AND</div> <div>scan_data/desc ></div> <div>Reset</div> </div>									
<div>Results</div> <div> <div>Manual Export</div> <div>Basic Raw Data</div> <div>Compare</div> <div>Total Results: 820881</div> <div>Results on current page: 100</div> </div>									
	origin_url	scan_data	ip	geoip.asn	htmltitle	html_body_undesp	favicon_md5	header_server	
<input type="checkbox"/>	http://ip22342.top	2025-06-25T20:20:48Z	202.79.173.213	152194	world-W02	WLeetHakBjocwMnOoh iGgRnMMygMyWb m92Cj4ChkxsoKx85	09840b77759d10eeaf1ff bf9332d4	cdn	Expand
<input type="checkbox"/>	http://ip22342.top	2025-06-25T20:20:48Z	202.79.173.213	152194	world-W02	WLeetHakBjocwMnOoh iGgRnMMygMyWb m92Cj4ChkxsoKx85	09840b77759d10eeaf1ff bf9332d4	cdn	Expand
<input type="checkbox"/>	http://ip22342.top	2025-06-25T20:20:47Z	202.79.173.213	152194	world-W02	WLeetHakBjocwMnOoh iGgRnMMygMyWb m92Cj4ChkxsoKx85	09840b77759d10eeaf1ff bf9332d4	cdn	Expand
<input type="checkbox"/>	https://kyukng50duel p	2025-06-25T20:20:42Z	27.104.32.4	152194	546.cc	IS3K-CHWetUdeBwTQ3w PUZvXfkwV7HvVdQgP u4eYMit6/jymM4k6rTS/ TPw-CHWw23wduhF4B4f vR8fHjgagpA4	09034c0985347ed478ce d330a05329a	AllyunOSS	Expand
<input type="checkbox"/>	https://whv207.cn	2025-06-25T20:20:36Z	134.122.136.104	152194	華康 站外链接识别!	IS3K-CHWetUdeBwTQ3w PUZvXfkwV7HvVdQgP u4eYMit6/jymM4k6rTS/ TPw-CHWw23wduhF4B4f vR8fHjgagpA4	09034c0985347ed478ce d330a05329a	CDNRay	Expand
<input type="checkbox"/>	http://034569.cc	2025-06-25T20:20:31Z	202.95.8.179	152194		3qVQ-c0b2QgFE8nD6c qpc0WCEBnz		cdn	Expand
<input type="checkbox"/>	http://034801.cc	2025-06-25T20:19:49Z	202.95.8.179	152194		3qVQ-c0b2QgFE8nD6c qpc0WCEBnz		cdn	Expand
<input type="checkbox"/>						W2gMUp9qhzZTreepae			

Silent Push Web Scanner ASN search with content filter results

According to Hurricane Electric, [ASN 152194](#) currently has 49 peers, with the majority out of Asia. But over the past year, our team observed that it averaged less than 15 peering partners. This type of new peering shift is rare and appears to indicate a new business strategy which could be occurring for a variety of reasons. One potential scenario is that ASN 152194 makes financial payments to its peering partners in a manner for which we currently lack visibility.



Screenshot of ASN 152194 peers

AS NUMBER: 214351

- **AS Name:** FEMOIT GB
- **Red Flags:** Unknown Website, Low IP Density, Temporary Email from Proton, Content Red Flags, Spamhaus Blocklist
- **Email Address:** hostdevbasx@proton[.]me
- **Details:** Femo IT Solutions has a domain but has never hosted any content on it. It merely hosts subdomains, such as mail.as214351.com, for its email inbox. The abuse email found through WHOIS RDAP for this ASN is currently a proton email: "hostdevbasx@proton[.]me." In August 2024, the ASN owner, "Femo IT Solutions," [registered the business in the U.K.](#) by an individual in Ukraine using a well-known U.K. business registration address also used by many others. This ASN is [recommended](#) for a block by Spamhaus with a documented 26-day average response time for abuse complaints.
 - Within Silent Push data, [ASN 214351](#) has fewer than 200 IPs mapped to it.
 - One way to parse what is hosted on a BPH is by searching for specific HTML title keywords, like "banking." On a normal ASN range, we would expect to find legitimate enterprise websites that mention "banking, investment, or crypto," whereas on a BPH, all or the majority of results with such keywords will be for websites featuring investment scams and the like.

Web Scanner ASN 214351 filtering on HTML title "Banking" query link

- `datasource = ["webscan"] AND geoip.asn = 214351 AND htmltitle = "*"Banking*"`

Menu Guide Search

Data Export

Threat Intelligence Management

Web Data

Web Scanner

Live Scan

WHOIS Data

DNS Data

Attack Surface Mapping

Brand Impersonation

Query History

Monitors

Advanced Query Builder

Sort order

ascn_data/ascn_v

Reset

Results

Manual Export

Basic Raw Data

Compare

Total Results: 20

Results on current page: 20

origin_url	ascn_data	ip	geolip.asn	hntitle	hntbody.ascexp	jarm	mlSHA256	path		
http://tqyq.digital	2025-05-24T07:21:38Z	180.178.189.22	214351	Banking-Princip der Finanzplanung unter Zie...	WZ2L20mONOPvZbP chRmUgawQJhA3B3P MQvXv5dyJc4agrcf Xvv3mWmdQwUwQ3Rf dS78ZkH-UUTVYMBot S	1832=webWmUd0d8 R00yUgMh8hGPTv8B DFUcAmryw8uJ/nU9P 999KvUwVdG5w8BDef rt			Expand	
http://t10wain.ch	2025-05-24T07:39:34Z	62.60.228.175	214391	Sendener Online Banking Login	WZ2L20mONOPvZbP chRmUgawQJhA3B3P MQvXv5dyJc4agrcf Xvv3mWmdQwUwQ3Rf dS78ZkH-UUTVYMBot S	2d3d2e00023d2e000 23d429d000000007f8d 2d6c0e69b0c5b818fe 4872386	A0:00:4D:F4:19:8B:1 6:3D:33:08:E8:00:E8:4 C:00:19:7B:75:1E:8:A A:19:50:3F:CA:02:4F:DB 54:3D		Expand	
https://tqyq.digital	2025-05-13T07:12:52Z	180.178.189.22	214351	Banking-Princip der Finanzplanung unter Zie...	WZ2L20mONOPvZbP chRmUgawQJhA3B3P MQvXv5dyJc4agrcf Xvv3mWmdQwUwQ3Rf dS78ZkH-UUTVYMBot S	21d45d6e000000409D F1d8A5d6e0000001G2D FdcUvL2duwYXFQFOW xwLc8T5Yf	ARFB2CFF5C96.CA d7E0587619DF.FC.9f 194D98DE87A248A A2C1005E5AF3A21W AB48		Expand	
https://ccofm-1d3d848299.com	2025-05-09T76:00:18Z	62.60.228.225	214351	LANDBANK (Access Retail Internet Banking - Login	WZ2L20mONOPvZbP chRmUgawQJhA3B3P MQvXv5dyJc4agrcf Xvv3mWmdQwUwQ3Rf dS78ZkH-UUTVYMBot S	21d45d6e000000409D F1d8A5d6e0000001G2D FdcUvL2duwYXFQFOW xwLc8T5Yf	ARFB2CFF5C96.CA d7E0587619DF.FC.9f 194D98DE87A248A A2C1005E5AF3A21W AB48		Expand	
https://ccofm-1d72d793.com	2025-05-07T70:55:02Z	62.60.228.225	214351	LANDBANK (Access Retail Internet Banking - Login	WZ2L20mONOPvZbP chRmUgawQJhA3B3P MQvXv5dyJc4agrcf Xvv3mWmdQwUwQ3Rf dS78ZkH-UUTVYMBot S	21d45d6e000000409D F1d8A5d6e0000001G2D FdcUvL2duwYXFQFOW xwLc8T5Yf	ARFB2CFF5C96.CA d7E0587619DF.FC.9f 194D98DE87A248A A2C1005E5AF3A21W AB48		Expand	

According to Hurricane Electric, [ASN 214351](#) has only 1 peering partner, AS30823 (aurologic GmbH).

AS NUMBER: 213194

- **AS Name:** NECHAEVDS-AS RU
- **Red Flags:** Unknown Website, Temporary Email on TutaMail, Low IP Density, Heavy DGA Usage
- **Domain:** Unknown
- **Email Address:** nechaevd12@tutamail[.]com
- **Details:** [ASN 213194](#) was allocated by IANA on February 19, 2025, and has an average of under eight IPs seen during June 2025, according to Silent Push data. For months, [Spamhaus](#) had no data about this ASN, with the first seen date being June 11, 2025. It is now reporting two IPs and two websites hosting malware.
- The first significant content Silent Push picked up on this ASN was in March 2025. Ever since, we've seen nearly 100% of the domains here using DGAs, which can be found with a simple query of the ASN.

[Web Scanner ASN query link](#)

- `datasource = ["webscan"] AND geoip.asn = 213194`

origin_url	scan_date	ip	geoip.asn	htmltitle	html_body_sadep	jarm	sslSHA256	path
http://1810wd.top	2025-04-25T09:30:52Z	193.37.69.98	213194		384A09a85d03a8bCh7A6PM8he+UA+PTNN6f0x0x5sewJ88waSE2jmcuK2WUW3W178xW5sewPm5z2WUW			/
http://1812wd.top	2025-04-25T09:21:02Z	193.37.69.98	213194		384A09a85d03a8bCh7A6PM8he+UA+PTNN6f0x0x5sewJ88waSE2jmcuK2WUW3W178xW5sewPm5z2WUW			/
http://1813wd.top	2025-04-25T09:16:18Z	193.37.69.98	213194	FASTPANEL	384A09a85d03a8bCh7A6PM8he+UA+PTNN6f0x0x5sewJ88waSE2jmcuK2WUW3W178xW5sewPm5z2WUW			/
http://1814wd.top	2025-04-25T09:10:57Z	193.37.69.98	213194		384A09a85d03a8bCh7A6PM8he+UA+PTNN6f0x0x5sewJ88waSE2jmcuK2WUW3W178xW5sewPm5z2WUW			/

Silent Push Web Scanner ASN search results

According to Hurricane Electric, [ASN 213194](#) has one peering partner, AS29182 (JSC IOT).

AS NUMBER: 215789

- **AS Name:** Karina Rashkovska
- **Red Flags:** Unknown Website, Temporary Email on Gmail, Heavy DGA Usage, No Live Infrastructure, Spamhaus Blocklist
- **Domain:** Unknown
- **Email Address:** karina.abusemailbox@gmail[.]com
- **Details:** [ASN 215789](#) was allocated in January 2024 by IANA. [Silent Push began monitoring this ASN](#) in February 2024, and it immediately started to contain primarily DGA domains. This ASN is recommended for a block on [Spamhaus](#) but shows no live IPs, and Silent Push hasn't seen active content here since April 2025. This is an example of a BPH that is not currently live but is still being tracked because if it acquires new IPs, it's likely to be quickly weaponized by its clients.

[Web Scanner ASN 215789 filter](#) showing no content since April 2025

- `datasource = ["webscan"] AND geoip.asn = 215789`

The screenshot displays the Silent Push Web Scanner interface. The query bar contains the search filter: `datasource = ["webscan"] AND geoip.asn = 215789`. The results table shows four entries, all with scan dates from April 2025 and no active content.

origin_url	scan_date	ip	geoip.asn	htmltitle	html_body_sdeeph
http://ord91236.live	2025-04-25T14:08:19Z	147.45.44.237	215789		12JJPLmRcHBLXSo/ GmORdopzQ+/jsAKIV UIQzEtEzAr040XX455 ZNMO99P5dzJjzmReL CWojYFtlAoH45HK69x i4
http://ldrs16959825.com	2025-04-25T13:12:08Z	147.45.44.237	215789		12JJPLmRcHBLXSo/ GmORdopzQ+/jsAKIV UIQzEtEzAr040XX455 ZNMO99P5dzJjzmReL CWojYFtlAoH45HK69x dz
http://lds347237837.com	2025-04-25T13:12:07Z	147.45.44.237	215789		12JJPLmRcHBLXSo/ GmORdopzQ+/jsAKIV UIQzEtEzAr040XX455 ZNMO99P5dzJjzmReL CWojYFtlAoH45HK69x w
http://ldrs458256781.com	2025-04-25T13:12:07Z	147.45.44.237	215789		12JJPLmRcHBLXSo/ GmORdopzQ+/jsAKIV UIQzEtEzAr040XX455 ZNMO99P5dzJjzmReL LCWojYFtlAoH45HK69

Silent Push Web Scanner ASN search shows no content since April 2025

Hurricane Electric aligns with Silent Push data and confirms that ASN 215789 has not been seen in global routing tables since June 3, 2025. Its previous active peer was AS30823 (aurologic GmbH).

AS NUMBER: 214943

- **AS Name:** RAILNET
- **Red Flags:** Unknown Domain, Temporary Email on Gmail, Spamhaus Blocklist, Content Red Flags
- **Domain:** Unknown
- **Email Address:** theodexer@gmail[.]com
- **Details:** [ASN 214943](#) was allocated by IANA in May 2024 and has fewer than 900 active IPs. There is no known domain associated with this ASN, and the abuse email address is from Gmail. Silent Push began to see content in September 2024, and almost immediately, most of the hosts were pushing scams or using DGA domains. [Spamhaus](#) recommends blocking the ASN and notes an average 7-day abuse response time.
- Searching for websites with an HTML title containing “Banking,” for example, provides us with a variety financial investment scams and no legitimate enterprise domains.

[Web Scanner ASN 214943 + HTML title filter for “Banking” search query link](#)

- `datasource = ["webscan"] AND geoip.asn = 214943 AND htmltitle = "**banking**"`

According to Hurricane Electric, [ASN 214943](#) has two peering partners: AS30823 (aurologic GmbH) and AS51396 (Pfcloud UG).

AS NUMBER: 34985

- **AS Name:** NETINNOVATIONLLC-AS-AP
- **Red Flags:** Temporary Email on Gmail, Low IP Density, Heavy DGA Usage, Spamhaus Blocklist
- **Domain:** netinnovation[.]net
- **Email Address:** gentandrew42@gmail[.]com
- **Details:** [ASN 34985](#) was allocated by IANA in 2019, but it’s still a very small host with less than 150 IPs active currently. Its website lacks significant details and appears to have not undergone a single update since 2022 ([Wayback Machine](#)). The use of a temporary Gmail account for its abuse response email is a red flag. [Spamhaus](#) suggests blocking this ASN and reports an 18-day abuse response time.
- Within the Silent Push data for this ASN, we see [nearly 8,000 scans in Web Scanner](#), but the majority of these are simply raw IPs serving content. If we [filter for only domain](#) scans on this ASN, there are fewer than 1k content captures. We can [search the live domains](#) for ones that include “API,” “admin,” or “login”—another way to filter for quality on an ASN—and we see that over 200 results feature one of these keywords, and everything here is a DGA domain that appears to be used for various types of scams.

Web Scanner ASN 34985 with domain filter for keywords API, Admin, or Login query link

- datasource = ["webscan"] AND geoip.asn = 34985 AND domain = ["*api*", "*admin*", "*login*"]

The screenshot shows the Web Scanner interface with the following details:

- Query:** `datasource = ["webscan"] AND geoip.asn = 34985 AND domain = ["*api*", "*admin*", "*login*"]`
- Sort order:** `scan_date/desc`
- Results:** Total Results: 203, Results on current page: 100
- Table Columns:** `origin_url`, `scan_date`, `ip`, `geoip.asn`, `htmltitle`, `html_body_sdeexp`
- Table Rows:**
 - `http://api2-edm-kcmsoft9922.com` | 2025-06-24T05:55:05Z | 185.254.240.99 | 34985 | IIS Windows Server | 12:B66QcIfVi+MYqGHwy090bEPLPX15exQ4xXEF9rDPOb0IjoWj:BGaq+MeHbeReuIPrTdU | Expand
 - `http://api-manager-log.com` | 2025-06-24T05:52:29Z | 45.135.48.229 | 34985 | IIS Windows Server | 12:B66QcIfVi+MYqGHwy090bEPLPX15exQ4xXEF9rDPOb0IjoWj:BGaq+MeHbeReuIPrTdU | Expand
 - `http://api-manager-77soft1235.com` | 2025-06-24T05:52:26Z | 185.254.240.99 | 34985 | IIS Windows Server | 12:B66QcIfVi+MYqGHwy090bEPLPX15exQ4xXEF9rDPOb0IjoWj:BGaq+MeHbeReuIPrTdU | Expand
 - `http://api-manager-log777.com` | 2025-06-24T05:51:32Z | 194.246.41.64 | 34985 | IIS Windows Server | 12:B66QcIfVi+MYqGHwy090bEPLPX15exQ4xXEF9rDPOb0IjoWj:BGaq+MeHbeReuIPrTdU | Expand
 - `http://api-manager-mantR000.com` | 2025-06-24T05:51:02Z | 185.254.240.138 | 34985 | IIS Windows Server | 12:B66QcIfVi+MYqGHwy090bEPLPX15exQ4xXEF9rDPOb0IjoWj:BGaq+MeHbeReuIPrTdU | Expand

According to Hurricane Electric, [ASN 34985](#) is a block "not managed by the RIPE NCC," but purportedly has seven peering partners, with three listed: AS17676 (SoftBank Corp.), AS9121 (Turk Telekomünikasyon Anonim Şirketi), and AS6939 (Hurricane Electric LLC).

AS NUMBER: 48589

- **AS Name:** SOW-A-AS UA (Also known as “Tiger Net”)
- **Red Flags:** Unknown Website, Temporary Email on GMAIL, Low IP Density, Heavy DGA Usage, Spamhaus Blocklist
- **Domain:** Unknown
- **Email Address:** imtigernet@gmail[.]com
- **Details:** [ASN 48589](#) was allocated by IANA in 2008 and has fewer than 600 active IP addresses as of 2025. There is no known domain for this ASN, and they use a Gmail address for handling abuse complaints. [Spamhaus](#) recommends blocking this ASN, but has only reported seeing one active IP address.
- [Silent Push DNS](#) data for this ASN indicates that the majority of domains appear to have been created using DGAs, and the [Web Scanner content for this ASN](#) confirms this observation. There is very little content on this ASN, and the small amount available appears to be part of DGA efforts or low-quality scams.

According to Hurricane Electric, [ASN 48589](#) has only 2 peering partners, AS55933 (Cloudie Limited) and AS134196 (ANYUN INTERNET TECHNOLOGY (HK) CO., LIMITED).

AS NUMBER: 49217

- **AS Name:** HOSTTYPE US
- **Red Flags:** Unknown Website, Temporary Email on Gmail, Suspicious Physical Address, Low IP Density, Spamhaus Blocklist, Heavy DGA Usage
- **Domain:** Unknown
- **Email Address:** hostypellc@gmail[.]com
- **Physical Address:** HostType LLC is registered at “30 N Gould St Ste R, Sheridan, WY 82801” ([Bizpedia](#)). It’s worth noting that Wyoming shell companies are frequently featured in global hacking attempts, as reported in [this 2023 Reuters piece](#).
- **Details:** [ASN 49217](#) was allocated by IANA in May 2023, has fewer than 20 IPs active, and a 30-day average IP density of about 3 IPs. Its domain is unknown, and it uses a Gmail address for receiving abuse complaints. [Spamhaus](#) recommends blocking this ASN; however, it is currently not tracking any associated IP addresses.
- Silent Push [Web Scanner data for ASN 49217](#) and our [PADNS data](#) both reveal a few unique domains, nearly all exhibit DGA patterns, and many of which have been online since 2024.

Menu Quick Search

Data Export
Threat Intelligence Management
Web Data
Web Scanner
Live Scan
WHOIS Data
DNS Data
Attack Surface Mapping
Brand Impersonation
Query History
Monitors
Advanced Query Builder

Simple Search
Advanced Search

My Searches
New
Save

Query
datasource = ["webscan"] AND geoip.asn = 49217 AND domain = "*,*"
Sort order
scan_date/asc
Reset

Results

Manual Export
Basic Raw Data
Compare
Total Results: 6479 Results on current page: 100

origin_url	scan_date	ip	geoip.asn	htmltitle	html_body_sdeeph
http://xteknoloji.net	2025-06-24T05:39:15Z	146.19.125.3	49217	xTeknoloji.net Linux Hosting, Sanel Sunucu ve Dedicated Server Çözümleri	768:dMzJE89i3UNUodLwEWV3hmm5i8SPwvErDnMthSs53y+nUoEV3hmm5nUS1H
http://yigitmetalhurdac.com	2025-06-24T05:23:54Z	146.19.125.3	49217	Yigit Metal Hurda - Esenyurt	768:93/b/nWMeZi7JnUkqid7WggdOimU63tQpOYgr8cH88pgqM7L6kmaqXOz/8jd7Fkh63tOpOvJZ8pgqM7GxwOz/
http://esecury.com	2025-06-24T05:20:08Z	146.19.125.2	49217	Welcome to nginx!	12:kxnp/awNFDvNbJw4xxebOR1KKCf0ktEjg+YjINQd30UINRVxWUOj:kRpnjbJwtsvXD05oP/l8kUIj7Wbj
http://xserver.tr	2025-06-24T05:18:36Z	146.19.125.3	49217	Domain Default page	192:KY6TUPW7YUdOxcPlbMW6XQ8Thb6nu43XOKxDVbidbv2Tms2uB0iUePyC8lv4RVgt:Yq9muRhigms2woCXLgdD3

The Silent Push Web Scanner ASN and domain search revealed new domains

According to Hurricane Electric, [ASN 49217](#) has only one peering partner, AS4867 (PENTECH BILISIM TEKNOLOJILERI SANAYI VE TICARET LIMITED SIRKETI).

AS NUMBER: 214940

- **AS Name:** KPROHOST LLC
- **Red Flags:** Unknown Website, Temporary Email on Gmail, Low IP Density, Heavy DGA Usage, Spamhaus Blocklist
- **Domain:** Unknown
- **Email Address:** kprohost.abuse@gmail[.]com
- **Details:** [ASN 214940](#) was allocated by IANA in May 2024, with Silent Push tracking fewer than 50 IPs active and a 30-day average of under 10 IPs. The website is unknown, and it uses a Gmail address to respond to abuse complaints. The ASN is listed on the [Spamhaus](#) blocklist with an 11-day abuse response time, but only two IPs are tracked.
- In the Silent Push [Web Scanner data](#), we have fewer than 2,000 scans from this ASN, and essentially everything appears malicious or uses a DGA domain. The same details can be seen in [our DNS data](#) for this ASN.

The screenshot displays the Silent Push Web Scanner interface. On the left is a sidebar with navigation options: Menu Quick Search, Data Export, Threat Intelligence Management, Web Data (selected), Web Scanner, Live Scan, WHOIS Data, DNS Data, Attack Surface Mapping, Brand Impersonation, Query History, Monitors, and Advanced Query Builder. The main panel has tabs for Simple Search and Advanced Search. The query bar contains: `datasource = ["webscan"] AND geoip.asn = 214940 AND domain = "*"."`. Below the query bar, the sort order is set to 'scan_date/desc'. The Results section shows a table with 100 results (Total Results: 1690). The table columns are: origin_uri, scan_date, ip, geoip.asn, htmltitle, and html_body_ssdeep. The first four rows of the table are highlighted with a green box:

origin_uri	scan_date	ip	geoip.asn	htmltitle	html_body_ssdeep
http://trakyx.com	2025-06-25T06:37:55Z	198.55.98.240	214940	MintCoin - Free \$25 Airdrop DeFi Platform	b1e11ipkxan/zjeivta+3a ozKagk6oPJ7QJb
http://brenger-be.com	2025-06-25T06:10:12Z	45.144.212.76	214940	Index of /	3:qVZxYvTG2sKEAEtv OqLzUbq5sWdVKZsN XADOFk2URCLZKqk3z :qzxYy2svAEsOqg8e2c uNXAD2UHqk3z
http://kazytokens.shop	2025-06-24T14:29:20Z	198.55.98.48	214940	KazyTokens	96:nBr+wgXveCUjulyM 8lhdsyTOIMA/eyFOV WPIUXc/SAF8mp4OV kiS7neBr+YXGCU5PM 8lh81MA/eyFOVWPIU X5Y
http://piracyisawesome.net	2025-06-24T14:10:31Z	45.144.212.99	214940	403 Forbidden	3:qVZxgROngsoMHXb vxL4AqWaMgs0U9CII TULLPpuNqz:qzxUigso CXLx0AqWDge0IlgLPuNqz

Everything appears malicious or uses a DGA domain in the Web Scanner search

According to Hurricane Electric, [ASN 214940](#) has only two peering partners: AS51396 (Pfcloud UG) and AS43641 (SOLLUTUM EU Sp z.o.o.).

AS NUMBER: 140224

- **AS Name:** SGPL-AS-AP STARCLOUD GLOBAL PTE. LTD. SG
- **Red Flags:** Heavy DGA Usage, Suspicious Physical Address, Content Red Flags
- **Domain:** as18186[.]com
- **Email Address:** abuse@nebulaglobal[.]net
- **Phone Number:** (970) 516-9999
 - This same phone number is also used by other hosting companies:
 - WAFCDn[.]com
 - SCGIDC @ www.scgidc[.]com
 - SafestWaf @ www.safestwaf[.]com
- **Physical Address:** 1359 S Drexel Way, Lakewood, CO 80232 ([Residential address according to Zillow](#))
- **Details:** [ASN 140224](#) was allocated by IANA in October 2024 and has over 3,000 IPs active and tracked by Silent Push. [Spamhaus](#) is not yet recommending a block and is tracking a 4-day abuse response time from 14 observed IP addresses. The website displays a Chinese logo and shares its phone number and business name with three other websites, all of which feature Chinese text. The address the business claims on its website is a residential address in Colorado.
- Silent Push has been tracking a significant amount of "[Triad Nexus](#)" threat actor infrastructure on this ASN - the same content we also tracked hosted on the FUNNULL CDN, which the U.S. Treasury [sanctioned](#) in May 2025. We have a complex query to share here, based on a combination of HTML, SHV, and server-based filters which makes it easy to surface content associated with assorted suspicious domains linked to Triad Nexus campaigns.

[Advanced Web Scanner Query with numerous filters and custom exclusions](#)

- `datasource = ["webscan"] AND geoip.asn = 140224 AND scan_date > "2025-03-01T01:31:19Z" AND htmltitle != "404 Not Found" AND htmltitle != "403 Forbidden" AND htmltitle != 404 AND htmltitle != "400 Invalid Hostname" AND htmltitle != "Sorry, the website has been stopped" AND body_analysis.SHV != "8bcd1e246ddf6c93cc6d8b4894" AND domain = "*. *" AND htmltitle != "导航" AND htmltitle != "504错误-回源网关超时" AND htmltitle != "Aladin Security 504 Error" AND htmltitle != "AccessDeny" AND header.server != "WAFCDN" AND header.server != "sudun" AND jarm != "3fd3fd0003fd3fd21c42d42d000000bdfc58c9a46434368cf60aa440385763" AND htmltitle != "盘古加速器官网" AND header.server != "Anti-CDN"`

Menu Quick Search

Data Export
Threat Intelligence Management
Web Data
Web Scanner
Live Scan
WHOIS Data
DNS Data
Attack Surface Mapping
Brand Impersonation
Query History
Monitors
Advanced Query Builder

datasource = ["webscan"] AND geoip.asn = 140224 AND scan_date > "2025-03-01T01:31:19Z" AND htmltitle != "404 Not Found" AND h

Sort order
scan_date/asc x
Reset

Results
1 2 3 4 5 ... 1406

Manual Export Basic Raw Data Compare
Total Results: 140574 Results on current page: 100

origin_url	scan_date	ip	geoip.asn	htmltitle	html_body_sadep
http://yengyi365.com	2025-06-26T23:17:28Z	206.119.23.104	140224		12kv/XLwOGOTONWwA5HVtBXxAAqJm0YevVy rC2H0whUHdWSGI5-ywR12WTHUHTbZGKJ; kyMNVv5HVTBxPtiVU VyOVwHSbuDcbOI
http://uhpvi.com	2025-06-26T23:15:59Z	206.119.22.10	140224	老王加速器_老王加速器 迅雷下载_一键链接全球 网络轻松上网	192:1AD0xnQIM3/M+M GWMDUBpFv8uSHrO +6n1kceH28WbDjyWp 91luhIDxnQP3/MIuyyF x8uSHkeeDjyYriuh
http://pinterest-lab.com	2025-06-26T23:15:00Z	206.119.18.239	140224	首页-竞技场-竞技宝网 站DOTA2.LOL.CSGO电竞 及体育赛事竞猜	192:YzOjx4letXqUNsQ 308yyysdntxd4GAkvG v7Mlb+IOOXd8oB6Wo DiverXqla40BLmfAKvG vy/28z
http://88888039.com	2025-06-26T23:14:45Z	206.119.30.108	140224		3072:slQDx9/Y4/c7BM rthpallqk66wc3wvOA vSC8bMy8Old2:IDv2sc7 BUppc66LKSC8eAo
http://progressiveeducationcenter.com	2025-06-26T23:14:16Z	206.119.21.5	140224	金蛙加速器_免费外网 加速器	192:ZScAD0xnQIMTU hMGIEMDuBIFn8uSH ZID6nblkHBQC8WzDjp p9WHL2ccodvnoPTU KTVlIFn8uSH/IBPDjHML2

Silent Push Web Scanner search for suspect Triad Nexus-associated domains

According to Hurricane Electric, [ASN 140224](#) has 28 peering partners, mostly based in Asia. In mid-June 2025, this ASN dropped from an average of over 70 peering partners to its current level of 28.

OTHER TYPES OF BULLETPROOF HOSTING

INFRASTRUCTURE LAUNDERING: THE NEXT STEP FOR BULLETPROOF HOSTING PROVIDERS

Silent Push [coined the phrase “Infrastructure Laundering”](#) to describe a growing criminal practice our analysts have observed where threat actors operating “hosting companies” rent IP addresses from mainstream hosting providers and map them to their criminal client websites.

Essentially, threat actors use what we call “account mules”—illicitly acquired cloud hosting accounts from vendors like Microsoft and Amazon—to ensure their malicious websites aren’t mapped to BPH IPs or suspicious ASNs in places like Russia and China which are regularly blocked en masse by defenders. By using U.S. IP space, websites mapped to these addresses also load more quickly for U.S. audiences.

Cloud providers then face a game of whack-a-mole in their attempts to take down these accounts as fast as they are being created and having their IPs mapped into CNAMEs that are further mapped into malicious domains. So, ultimately, if you know the CNAMEs being used in the DNS setup, you can track both the malicious client websites and the IP addresses being mapped into the infrastructure, which includes the stolen IPs via infrastructure laundering. For more detailed information, refer to our [public blog on Infrastructure Laundering](#).

Important note: While our team at Silent Push has been tracking this specific scheme for well over a year, there has thus far been minimal public reporting on the specific defenses being deployed by cloud providers or the impacts to consumers who are losing money on the malicious pig butchering investment scam websites hosted using U.S. IP addresses outside of the sanctions notice by the [US Treasury](#).

INFRASTRUCTURE LAUNDERING



1. SERVICES NEEDED

Threat actors search for space to host and hide their malicious sites.



2. SMOKESCREENS DEPLOYED

Intermediaries such as CDNs “launder” their infrastructure by hosting it within large, legitimate Cloud platforms.



3. EXECUTION

Intermediaries use CNAME mapping and DNS techniques to link criminal websites to IPs of credible hosts, legitimizing their hosting services.



4. OBFUSCATION

Intermediaries profit by masking origins and intent, creating an illusion of legitimacy for unsuspecting visitors.



5. ANONYMITY ACHIEVED

Criminals exploit CDNs that host legitimate businesses, complicating takedowns and blocking without disrupting valid web traffic.

Learn more: www.silentpush.com/blog



Silent Push Infrastructure Laundering infographic

DYNAMIC DNS (DDNS) PROVIDERS CREATE BPH-LIKE NETWORKS

Dynamic DNS vendors (also known as providers of “Publicly Rentable Domains”) are essentially service providers who rent out subdomains for the domains they control and automatically map DNS records to those rented subdomains. Some premium Dynamic DNS services allow for customization of these DNS records; however, this is not typical of how this kind of infrastructure is usually set up.

A large number of enterprise hosts that provide these subdomain rental services can be found on the “[Public Suffix List](#)” (PSL). Browser developers use this list for security purposes in order to ensure that subdomains on the list can’t read cookies for other subdomains or the root domain, essentially creating the same types of cookie logic seen across unique domains.

The PSL is also used for a variety of internet products and services, and is regularly updated. However, it has restrictions on the addition of new domains. Only a verified domain owner can add their domain to the Public Suffix List, which means that in practice, there are no community submissions to the list. Therefore, tens of thousands of dynamic DNS domains and publicly rentable domains are not included in the PSL.

Dynamic DNS and publicly rentable domain services, such as afraid[.]org, offer a massive number of available domains. Afraid has over [22,000 domains with subdomains for rent](#), and only a tiny fraction are on the PSL.

Thus, there are myriad examples of serious threat actors using publicly rentable domains/dynamic DNS domain services in their attacks. Some of the more notable examples include:

- In 2025, [TA406 was using a dynamic DNS provider](#) from mygamesonline[.]org in attacks targeting entities in Ukraine.
- In 2014, Microsoft [led efforts to take over some](#) of the No-IP Dynamic DNS Domains that were heavily used in ongoing attacks.
- In 2019, [Chinese APT10 was observed](#) using Dynamic DNS domains by Rewterz.
- APT Group Gallium was [documented in 2022 by Palo Alto Networks](#) using Dynamic DNS domains.
- In 2022, Google Mandiant [reported that APT29 was exclusively using Dynamic DNS domains](#) for its QUIETEXIT C2 domains.
- APT33 was cited as using custom domains as well as Dynamic DNS domains [in a September 2023 report](#) from Booz Allen.
- Security researcher “Gi7w0rm” [demonstrated in a September 2023 report](#) that the DDGroup threat actor heavily utilized Dynamic DNS domains for C2 communications.
- APT28 (Fancy Bear) was noted [in a 2024 FBI report](#) to have heavily used Dynamic DNS domains.
- DarkComet Malware was [reported by Hyas in August 2024 to be heavily deployed into Dynamic DNS domains](#).
- Scattered Spider used a publicly rentable domain in a January 2025 campaign, detailed in our exclusive March 2025 enterprise customer report.
- Gamaredon has previously been observed using Dynamic DNS domains, as highlighted in our exclusive May 2025 enterprise customer report.

Numerous companies track the abuse takedown speed of ASNs and hosts, but few track the abuse takedown speed of services that rent subdomains on specific services.

Many Dynamic DNS providers also lack a clear method by which to submit abuse complaints and/or do not have a clear commitment to, nor track record of, taking action.

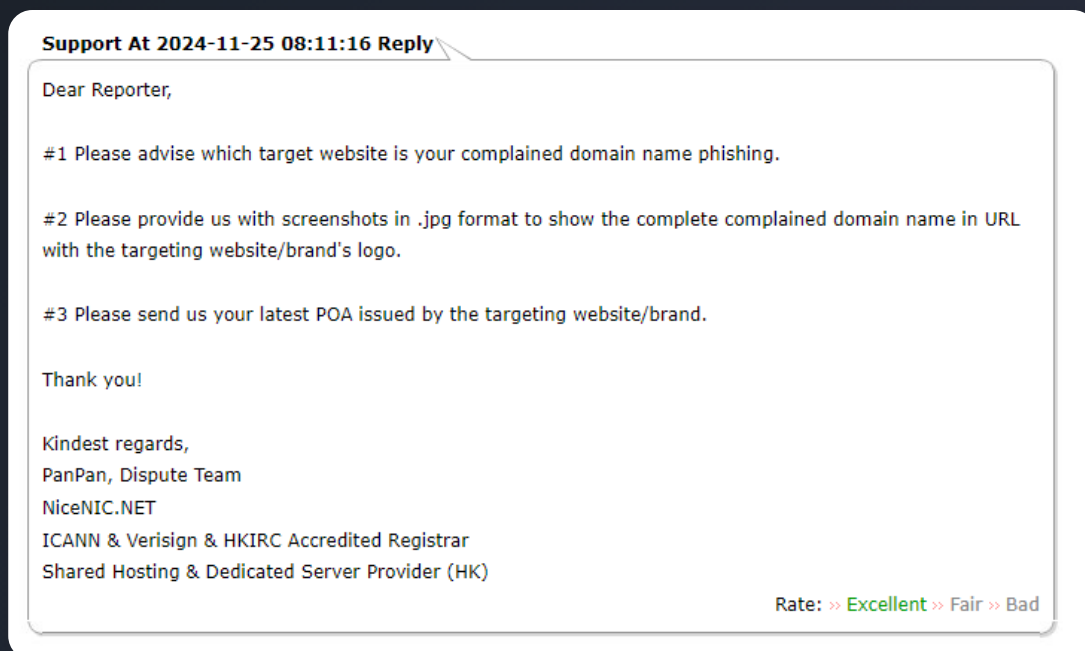
Silent Push tracks tens of thousands of these domains, and we believe organizations serious about their security should always be alerting on connections to these domains and consider, in some instances, blocking all connections to them.

BULLETPROOF REGISTRAR: NICE NIC

NiceNIC (nicens[.]net) has grown to become the domain registrar of choice for numerous threat actors, including Scattered Spider and other threat groups associated with [The Com](#), the international online network of threat actors who have been behind some of the most widely-reported hacks against large organizations over the last several years. Silent Push has reported on several of these groups in our [public blogs](#), with additional details for each kept in reporting only available to our enterprise customers.

This registrar exhibits some obvious red flags (such as a Hong Kong headquarters and a lackadaisical approach to responding to abuse complaints), but Silent Push Threat Analysts primarily refer to NiceNIC as a “Bulletproof Registrar” because the service requires a “Power of Attorney” (POA) over a website or brand to submit a successful abuse takedown request.

This provision—one that is virtually unheard of in most other takedown scenarios—is even directly referenced in NiceNIC’s generic response to abuse complaints, as seen below.



Screenshot of NiceNIC dispute team email

The process of requiring a POA over a brand to submit a takedown request means that if a threat actor abuses dozens of brands with unique scams or phishing sites, defenders would need to exert a Herculean effort to obtain the necessary legal permission from all the impacted brands to complete the takedown process. Meanwhile, there's a slim likelihood that major brands have the resources or labyrinthine knowledge necessary to successfully combat NiceNIC-registered content targeted at them.

In effect, thanks to this provision, domains registered on NiceNIC typically end up staying online for far longer than domains registered on other providers.

INCREASING PRESSURE ON BPH PROVIDERS USING GOVERNMENT SANCTIONS

Cybercriminals have long had the upper hand; moving faster, adapting quicker, and exploiting gaps in global enforcement's ability to respond. But BPH operators are starting to see that advantage erode.

In February 2025, for example, we saw a rare example of cross-government collaboration against an online threat when the U.S., Australia, and the U.K. [issued joint sanctions](#) against "Zservers" (also known as "Xhost"), a Russian BPH service provider. Dutch outlet Politie [reported](#) that a total of 127 servers were taken offline and seized due to their involvement in ransomware and botnet operations.



[Source Politie](#): Screenshot of confiscated Zservers equipment

While this isn't the first time sanctions have been issued against BPH services, we've only seen sporadic victories against malicious hosting companies and BPH providers thus far. Some recent, notable examples of this include:

- In July 2022, the [United States Attorney for the Southern District of New York announced](#) that the threat actor nicknamed "Virus" had been extradited to the U.S. for his role in hosting a prominent BPH company.
- In August 2023, the [DOJ indicted](#) the admin of BPH company, LolekHosted, that had operated the host for nearly a decade, including hosting dozens of NetWalker ransomware instances used in attacks.
- In May 2025, FUNNULL, a Philippines-based Infrastructure Laundering service, and its [administrator Lizhi Liu](#) were [sanctioned](#) by the U.S. Treasury Department for facilitating a ring of fraudulent investment websites (specifically for virtual currencies). Authorities reported that these websites had collectively defrauded U.S. consumers of over \$200 million - with average victims losing roughly \$150,000 each.
- Also in May 2025, Stark Industries, a web host that was hosting [significant FIN7 infrastructure](#) but had responded to abuse complaints, was [sanctioned by the Council of the EU](#) for "acting as enablers of various Russian state-sponsored and affiliated actors to conduct destabilising activities, including information manipulation, interference, and cyber-attacks against the Union and third countries."
- In July 2025, a BPH provider known as [Aeza Group](#), a BPH provider, was sanctioned by the U.S. Treasury for its role in supporting global criminal activity.

We encourage the U.S. government and other major governments to create and maintain ongoing processes within their relevant cybersecurity agencies to review BPH service providers, as well as cooperate with the private sector when it comes to imposing financial sanctions on bad actors and repeat offenders. Agencies working on these issues need ongoing financial resources to support these types of efforts if there's to be any hope of sanctions seeing success against those providers who have been allowed to operate in this space.

Often, there are also few legal or punitive ramifications for the companies who support these networks by providing “peering” services, which are often exploited to route malicious traffic between these networks. Trite as it sounds, these services are more or less exploiting the “[series of tubes](#)” that make up the modern internet, and rarely face consequences commensurate with the role they are playing in keeping these services online. We encourage law enforcement worldwide to not only track BPH providers and illicit hosting companies, but also identify those companies who act as support scaffolding to their operations via peering.

Through extended public and private sector collaboration, defenders can more closely track the evolution of these shady practices, and take steps to resolve this complex, ongoing problem.

Real progress starts with awareness. Our team believes that the more attention this issue receives, the closer law enforcement, organizations, and the defenders who support them get to real solutions.

BULLETPROOF HOSTING IS EXPANDING, NOT GOING AWAY

“Bulletproof Hosting” has become both a marketing term used by various aggressive hosting companies and a reality of malicious infrastructure that shows no signs of going away. Many internet-based organizations appear to revel in their efforts to prevent “censorship” and, undercutting the credible arguments for privacy that exist, treat the hosting of illegal content as a badge of honor.

Furthermore, the lack of regulations from ICANN and regional domain authorities continue to make it relatively easy for bulletproof hosts to acquire entire ASN ranges, leaving their resolution a murky policy issue that has gone unresolved.

With the emergence of new concepts like Infrastructure Laundering and the rise of “Bulletproof Registrars,” threat actors are demonstrating their ability and willingness to adopt new techniques.

We encourage organizations, agencies, and law enforcement interested in combatting these techniques to reach out to us and make use of the powerful capabilities we’ve developed in our platform to arm defenders with.

Silent Push is committed to protecting its customers and the broader community. Our extensive and constantly updated IOFA™ feeds cover Bulletproof Hosting, Infrastructure Laundering efforts, and more, offering our enterprise clients the very best in preemptive detection and defense.

Our team also hopes that, by presenting this white paper and the concepts contained within, we can educate our fellow defenders and push these important conversations forward.



ABOUT SILENT PUSH

Silent Push is the only cybersecurity platform that offers **Indicators Of Future Attack (IOFA)**[™] – domains and IPs which are yet to be fully deployed in an attack, including assets initiated during the reconnaissance and weaponization phases. **IOFA**[™] allow teams to track patterns in attacker DNS automation, that show where the next digital assault will originate from.

Utilize preemptive intelligence—not available anywhere else—to expose malicious intent and infrastructure early, so that your organization's incident response (IR), SOC, and defensive teams can act swiftly to shut the doors before attackers can gain access.

LEVEL-UP YOUR SIEM AND SOAR WORKFLOWS

- Utilize a range of native integrations that connect Silent Push data with industry-leading SIEM, SOAR, and TIP platforms. Automate downstream actions that reduce manual intervention, and provide fast, reliable context on unknown indicators in your alert queues.

TAKE ADVANTAGE OF OUR ROBUST INTEGRATIONS

- Use a Silent Push Enterprise subscription to feed enriched threat data into your existing security stack using a suite of 100+ domain, IPv4/6 and URL endpoints. Enrich your organization's threat hunting and detection operations with risk and reputation scoring tailored to your unique requirements.

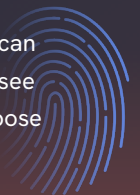
UNLOCK THE SILENT PUSH CHROME EXTENSION

- Our integrated Chrome extension allows Enterprise Edition users with an API key to scan, extract, save, and analyze DNS data in Silent Push directly from a web browser, including URLs, domains, and IPs.
 - Instantly flag indicators in **IOFA**[™] Feeds and receive risk scores.
 - Extract DNS records and WHOIS data directly from any webpage.
 - One-click pivot into the Silent Push platform for live and historical scans.



PREEMPTIVE CYBER DEFENSE WITH
INDICATORS OF FUTURE ATTACK[™]

Book a demo with us to see how Silent Push can help you stop threats before they strike and see how **Indicators Of Future Attack (IOFA)**[™] expose adversary infrastructure as it's being set up.



[REQUEST A DEMO](#)

Legal Disclaimer: This white paper is provided for informational purposes only and reflects the results of Silent Push, Inc.'s own research, analysis, and assumptions as of the date of publication. The findings, conclusions, and opinions expressed have not been independently verified, audited, or reviewed by any third party and may be subject to change without notice. Silent Push, Inc. makes no representation or warranty, express or implied, as to the accuracy, completeness, or fitness for any particular purpose of the information contained herein, and disclaims any liability for reliance on this white paper. This document does not constitute investment, legal, tax, or other professional advice.